

Приложение 4  
к основной профессиональной образовательной программе  
по направлению подготовки 10.04.01 Информационная  
безопасность направленность (профиль) программы Защита  
информационного пространства субъектов экономической  
деятельности

**Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Российский экономический университет имени Г.В. Плеханова»**

**Институт математики, информационных систем и цифровой экономики**

**Кафедра Прикладной информатики и информационной безопасности**

## **ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ**

### **Б2.В.01(П) Проектно-технологическая практика**

<b>Направление подготовки</b>	<b><u>10.04.01 Информационная безопасность</u></b>
<b>Направленность (профиль) программы</b>	<b><u>Защита информационного пространства субъектов экономической деятельности</u></b>
<b>Уровень высшего образования</b>	<b><u>Магистратура</u></b>

Год начала подготовки – 2022

Москва, 2022 г.

Составитель: \_\_\_\_\_ / Сизов В.А., д.т.н., профессор, каф. ПИиИБ /

Программа практики одобрена на заседании кафедры Прикладной информатики и информационной безопасности, протокол № 10 от «28» апреля 2021 г.

Заведующий кафедрой \_\_\_\_\_ / Тельнов Ю.Ф. д.э.н., профессор /  
(подпись)

## СОДЕРЖАНИЕ

1. ЦЕЛИ ПРАКТИКИ .....	4
2. ЗАДАЧИ ПРАКТИКИ.....	4
3. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ .....	5
4. ВИД И ТИПЫ ПРОВЕДЕНИЯ ПРАКТИКИ .....	5
5. МЕСТО И ВРЕМЯ ПРОВЕДЕНИЯ ПРАКТИКИ.....	5
6. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ТРЕБУЕМЫМИ ИНДИКАТОРАМИ ДОСТИЖЕНИЯ КОМПЕТЕНЦИЙ И КОМПЕТЕНЦИЯМИ ВЫПУСКНИКОВ.....	5
7. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ .....	29
8. ОБРАЗОВАТЕЛЬНЫЕ, НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЕ И НАУЧНО-ПРОИЗВОДСТВЕННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ НА ПРАКТИКЕ .....	33
9. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ НА ПРАКТИКЕ .....	33
10. ФОРМЫ ОТЧЕТНОЙ ДОКУМЕНТАЦИИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ .....	33
11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ.....	34
12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ.....	34
13. ОБЯЗАННОСТИ ОБУЧАЮЩЕГОСЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ .....	37
14. ОБЯЗАННОСТИ РУКОВОДИТЕЛЯ ПРАКТИКИ .....	37
15. ОЦЕНОЧНЫЕ СРЕДСТВА .....	37
16. ОСОБЕННОСТИ ПРОХОЖДЕНИЯ ПРАКТИКИ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ.....	76
ПРИЛОЖЕНИЕ 1.....	77

## 1. Цели практики

Практика студентов магистратуры по направлению 10.04.01 «Информационная безопасность» направленность (профиль) программы «Защита информационного пространства субъектов экономической деятельности» является составной частью основной образовательной программы и обеспечивает связь теоретического обучения с практической деятельностью, придавая процессу обучения прикладную направленность.

Целью производственной практики: проектно-технологической практики является: подготовка магистра к решению задач предприятия в области информационной безопасности, сбор материала для выполнения выпускной квалификационной работы магистранта.

## 2. Задачи практики

Задачами проектно-технологической практики являются:

- Ознакомление с:

- историей, традициями и задачами деятельности подразделений субъектов экономической деятельности (СЭД);
- процессом выполнения научных исследований и производственных задач в области защиты информационного пространства СЭД;
- методами планирования и проведения мероприятий по защите информационного пространства СЭД;
- с новыми методологиями и технологиями проектирования защищенных информационных систем (ИС);
- с новыми инструментами и методами управления проектами защищенных ИС;
- технологиями интеграции средств защиты информации (СЗИ) с существующими СЗИ у заказчика.

- Изучение:

- аудита конфигураций СЗИ в проектах любого уровня сложности СЭД;
- структурных и функциональных схем СЭД;
- организации деятельности подразделений защиты информации СЭД;
- порядка и методов ведения делопроизводства в области информационной безопасности на предприятии;
- методик выполнения аналитических работ в области информационной безопасности СЭД;
- регламентов и процедур управления проектами СЗИ.

- Приобретение практических навыков:

- выполнения функциональных обязанностей научного сотрудника, специалиста;
- разработки новых инструментов и методов управления проектами;
- сопровождения системы защиты информации СЭД и поддержания его функциональных характеристик в заданных пределах;
- анализа инцидентов информационной безопасности;
- подготовка предложений по новым инструментам и методам управления информационной безопасностью;
- проведения приемо-сдаточных испытаний (валидации) в проектах любого уровня сложности в области защиты информационного пространства СЭД.

- Выполнение индивидуальных заданий.

- Подготовка и защита отчета по практике.

### 3. Место практики в структуре образовательной программы

Раздел образовательной программы подготовки магистров «Практика» является обязательным и представляет собой вид учебных занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся.

Проектно-технологическая практика реализуется в части, формируемой участниками образовательных отношений Блока 2 «Практика».

Практика вырабатывает умения и практические навыки, приобретаемые обучающимися в результате освоения теоретических дисциплин блока Б1, способствует комплексному формированию универсальных и профессиональных компетенций у обучающихся.

### 4. Вид и типы проведения практики

4.1. Вид практики – производственная.

4.2. Тип практики - проектно-технологическая практика.

### 5. Место и время проведения практики

#### **Место проведения практики:**

- непосредственно в Университете, в том числе в структурном подразделении Университета, предназначенном для проведения практической подготовки;
- в организации, осуществляющей деятельность по профилю соответствующей образовательной программы, в том числе в структурном подразделении профильной организации, предназначенном для проведения практической подготовки на основании договора/соглашения о сотрудничестве, заключаемого между Университетом и профильной организацией;
- по месту трудовой деятельности, если профессиональная деятельность, осуществляемая обучающимися, соответствует требованиям образовательной программы к проведению практики и заключен индивидуальный договор на практическую подготовку.

Руководство практикой осуществляется преподавателями кафедры Прикладной информатики и информационной безопасности совместно со специалистами профильных организаций.

Обучающиеся по согласованию с руководителем практики от Университета, могут избрать иное учреждение, или организацию - место прохождения практики. В этом случае обучающиеся получают от руководителя из числа ППС Университета индивидуальное задание.

**Время проведения практики:** в соответствии с учебным планом по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) программы «Защита информационного пространства субъектов экономической деятельности», практика проводится в 4 семестре.

**Практическая подготовка** обучающихся с ограниченными возможностями здоровья и инвалидов организуется с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

### 6. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с требуемыми индикаторами достижения компетенций и компетенциями выпускников

В результате прохождения проектно-технологической практики у обучающихся должны быть сформированы элементы следующих компетенций в соответствии с ФГОС ВО по

направлению подготовки 10.04.01 «Информационная безопасность», с учетом обобщенных трудовых функций профессионального стандарта, к выполнению которых в ходе практики готовится обучающийся: УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций (код и наименование индикатора)	Результаты обучения (знания, умения)
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Анализирует проблемную ситуацию как целостную систему, выявляя ее составляющие и связи между ними	УК-1.1. З-1. <b>Знает</b> методику постановки цели и определения способов ее достижения
		УК-1.1. У-1. <b>Умеет</b> определить суть проблемной ситуации и этапы ее разрешения с учетом вариативных контекстов
		УК-1.1. У-2. <b>Умеет</b> осуществлять сбор, систематизацию и критический анализ информации, необходимой для выработки стратегии действий по разрешению проблемной ситуации
	УК-1.2. Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации	УК-1.2. У-1. <b>Умеет</b> Проводит оценку адекватности и достоверности информации о проблемной ситуации, умеет работать с противоречивой информацией из разных источников
		УК-1.2. У-2. <b>Умеет</b> Осуществляет поиск решений проблемной ситуации на основе действий, эксперимента и опыта
		УК-1.2. У-3. <b>Умеет</b> Критически оценивает возможные варианты решения проблемной

		ситуации на основе анализа причинно-следственных связей
	УК-1.3. Вырабатывает стратегию действий для решения проблемной ситуации в виде последовательности шагов, предвидя результат каждого из них	УК-1.3. У-1 <b>Умеет</b> . Осуществляет и аргументирует выбор стратегии по решению проблемной ситуации, оценивает преимущества и недостатки выбранной стратегии
		УК-1.3. У-2. <b>Умеет</b> Осуществляет разработку плана действий по решению проблемной ситуации, определяет и оценивает практические последствия реализации действий по разрешению проблемной ситуации
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Понимает принципы проектного подхода к управлению	УК-2.1. З-1. <b>Знает</b> основные методологические подходы в сфере управления проектами
		УК-2.1. З-2. <b>Знает</b> методы и модели структуризации проекта
		УК-2.1. З-3. <b>Знает</b> методы управления рисками проекта на всех стадиях его жизненного цикла
		УК-2.1. У-1. <b>Умеет</b> строить и структурировать жизненный цикл проекта
		УК-2.1. У-2. <b>Умеет</b> Применяет основные процедуры и методы управления проектами и подготовки проектных решений
	УК-2.2. Демонстрирует способность управления проектами	УК-2.2. З-1. <b>Знает</b> основные виды проектов их специфику и особенности управления ими

		<p>УК-2.2. 3-2. <b>Знает</b> способы оценки проектов с учетом факторов риска и неопределенности</p>
		<p>УК-2.2. 3-3. <b>Знает</b> основные принципы управления проектами на всех стадиях жизненного цикла</p>
		<p>УК-2.2. У-1. <b>Умеет</b> планировать реализацию проекта</p>
		<p>УК-2.2. У-2. <b>Умеет</b> оценивать эффективности проектов</p>
		<p>УК-2.2. У-3. <b>Умеет</b> измерять и анализировать результаты проектной деятельности</p>
<p>УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели</p>	<p>УК-3.1. Понимает и знает особенности формирования эффективной команды</p>	<p>УК-3.1. 3-1. <b>Знает</b> основные модели командообразования и факторы, влияющие на эффективность командной работы</p>
		<p>УК-3.1. 3-1. <b>Знает</b> основные модели командообразования и факторы, влияющие на эффективность командной работы</p>
		<p>УК-3.1. 3-3. <b>Знает</b> основные современные технологии организации деятельности команд, в том числе - виртуальных</p>
		<p>УК-3.1. У-1. <b>Умеет</b> определять роль каждого участника команды</p>
		<p>УК-3.1. У-2. <b>Умеет</b> ставить перед каждым участником команды четко сформулированную задачу с учетом его роли</p>

		<p>УК-3.1. У-3. <b>Умеет</b> выбирать методы организации работы команды с учетом специфики поставленной цели, временных и прочих ограничений</p>
		<p>УК-3.1. У-4. <b>Умеет</b> составлять планы и графики основных шагов по достижению поставленной перед командой цели и оценивать необходимые временные, информационные и другие ресурсы</p>
	<p>УК-3.2. Демонстрирует поведение эффективного организатора и координатора командного взаимодействия</p>	<p>УК-3.2. З-1. <b>Знает</b> основные методы анализа взаимодействия в команде</p>
		<p>УК-3.2. З-2. <b>Знает</b> основные современные технологии коммуникации различного типа</p>
		<p>УК-3.2. З-3. <b>Знает</b> принципы предоставления обратной связи</p>
		<p>УК-3.2. У-1. <b>Умеет</b> поддерживать в команде атмосферу сотрудничества и достижения цели, показывая ценность вклада каждого участника</p>
		<p>УК-3.2. У-2. <b>Умеет</b> предоставлять эффективную обратную связь участникам команды по промежуточным и конечным результатам работы</p>
		<p>УК-3.2. У-3. <b>Умеет</b> выявлять конфликты, возникающие в процессе командной работы, и конструктивно управлять ими</p>

		УК-3.2. У-4. <b>Умеет</b> использовать различные типы коммуникации для обеспечения эффективного взаимодействия участников команды, в том числе - виртуальной
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Составляет в соответствии с нормами государственного языка РФ и иностранного языка документы (письма, эссе, рефераты и др.) для академического и профессионального взаимодействия	УК-4.1. З-1. <b>Знает</b> методы и способы применения информационно-коммуникационных технологий для сбора, хранения, обработки, представления и передачи информации в ситуациях академического и профессионального взаимодействия
		УК-4.1. У-1. <b>Умеет</b> Самостоятельно находит и обрабатывает информацию, необходимую для качественного выполнения академических и профессиональных задач и достижения профессионально значимых целей, в т.ч. на иностранном языке
		УК-4.1. У-2. <b>Умеет</b> Составляет, редактирует на государственном языке РФ и/или иностранном языке, выполняет корректный перевод с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный язык различных академических и профессиональных текстов
	УК-4.2. Представляет результаты академической и	УК-4.2. З-1. <b>Знает</b> основные концепции организации

	<p>профессиональной деятельности на мероприятиях различного формата, включая международные</p>	<p>межличностного взаимодействия в информационной среде</p>
		<p><b>УК-4.2. У-1. Умеет</b>  Владеет навыками и умениями установления и развития академических и профессиональных контактов, в т.ч. в международной среде, в соответствии с целями, задачами и условиями совместной деятельности, включая обмен информацией и выработку единой стратегии взаимодействия</p>
		<p><b>УК-4.3. У-1. Умеет</b>  Воспринимает и анализирует информацию на государственном языке РФ и иностранном языке в процессе академического и профессионального взаимодействия</p>
	<p><b>УК-4.3. У-2. Умеет</b>  Принимает участие в академических и профессиональных дискуссиях на государственном языке РФ и/или иностранном языке, аргументированно отстаивая свои позиции и идеи</p>	
<p><b>УК-5.</b> Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия</p>	<p><b>УК-5.1.</b> Имеет представление о сущности и принципах анализа разнообразия культур в процессе межкультурного взаимодействия</p>	<p><b>УК-5.1. З-1. Знает</b>  принципы анализа и учета разнообразия культур в процессе межкультурного взаимодействия</p>
		<p><b>УК-5.1. З-2. Знает</b>  методы анализа и учета разнообразия культур в процессе межкультурного взаимодействия</p>
		<p><b>УК-5.1. З-3. Знает</b></p>

		нормы межкультурного взаимодействия с учетом разнообразия культур
	УК-5.2. Демонстрирует способность анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.2. У-1. <b>Умеет</b> анализировать разнообразие культур в процессе межкультурного взаимодействия
		УК-5.2. У-2. <b>Умеет</b> учитывать разнообразие культур в процессе межкультурного взаимодействия
		УК-5.2. У-3. <b>Умеет</b> строить межкультурное взаимодействие с учетом разнообразия культур
УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1. Определяет стимулы, мотивы и приоритеты собственной профессиональной деятельности и цели карьерного роста	УК-6.1. З-1. <b>Знает</b> основные принципы мотивации и стимулирования карьерного развития
		УК-6.1. З-2. <b>Знает</b> способы самооценки и самоопределения
		УК-6.1. У-1. <b>Умеет</b> оценить возможности реализации собственных профессиональных целей и расставить приоритеты
	УК-6.2. Проводит рефлексию своей деятельности и разрабатывает способы ее совершенствования	УК-6.2. У-1. <b>Умеет</b> провести анализ результатов своей социальной и профессиональной деятельности
УК-6.2. У-2. <b>Умеет</b> корректировать планы личного и профессионального развития		
ПК-1. Обеспечение информационной безопасности вычислительных сетей	ПК-1.1. Анализирует основные характеристики и возможности телекоммуникационных	ПК-1.1. З-1. <b>Знает</b> основные типы и характеристики сетевого оборудования отечественных и ведущих мировых производителей

	систем по передаче информации	ПК-1.1. У-1. <b>Умеет</b> осуществлять подбор сетевого оборудования для конкретных организаций и эксплуатировать сетевое оборудование
	ПК-1.2. Проектирует и реализует политику безопасности вычислительных сетей	ПК-1.2. З-1. <b>Знает</b> основные методологии проектирования политик информационной безопасности вычислительных сетей
		ПК-1.2. У-1. <b>Умеет</b> разрабатывать и реализовывать политики работы в корпоративных сетях, проектировать и эксплуатировать локальные вычислительные сети, восстанавливать их работоспособность
ПК-2. Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	ПК-2.1. Разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем	ПК-2.1. З-1. <b>Знает</b> нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
		ПК-2.1. У-1. <b>Умеет</b> разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД
	ПК-2.2. Применяет средства схемотехнического проектирования и современную	ПК-2.2. З-1. <b>Знает</b> принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и

	измерительную аппаратуру	блоков электронной аппаратуры
		ПК-2.2. У-1. <b>Умеет</b> проводить комплексное тестирование аппаратных и программных средств
	ПК-2.3. Синтезирует структурные и функциональные схемы защищенных автоматизированных систем	ПК-2.3. З-1. <b>Знает</b> основные информационные технологии, используемые в автоматизированных системах
		ПК-2.3. У-1. <b>Умеет</b> оценивать сложность алгоритмов и вычислений
	ПК-2.4. Разрабатывает программное обеспечение, технические средства, базы данных и компьютерные сети с учетом требований по обеспечению защиты информации	ПК-2.4. З-1. <b>Знает</b> современные технологии программирования, особенности защиты информации в автоматизированных системах управления технологическими процессами
		ПК-2.4. У-1. <b>Умеет</b> разрабатывать программное обеспечение, технические средства, базы данных и компьютерные сети с учетом требований по обеспечению защиты информации
	ПК-2.5. Разрабатывает электронные схемы с учетом требований по защите информации автоматизированных и информационных систем	ПК-2.5. З-1. <b>Знает</b> принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры
		ПК-2.5. У-1. <b>Умеет</b> осуществлять мониторинг и оперативное устранение уязвимостей в программном и аппаратном обеспечении, выявлять уязвимости в

		программном и аппаратном обеспечении
	ПК-2.6. Оптимизирует работу электронных схем с учетом требований по защите информации	ПК-2.6. 3-1. <b>Знает</b> методы оптимизации схемотехнических решений
		ПК-2.6. У-1. <b>Умеет</b> оценивать сложность алгоритмов и вычислений
ПК-3. Обоснование необходимости защиты информации в автоматизированной системе	ПК-3.1. Анализирует характер обрабатываемой информации и определяет перечень информации, подлежащей защите	ПК-3.1. 3-1. <b>Знает</b> виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах
		ПК-3.1. У-1. <b>Умеет</b> классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации
	ПК-3.2. Выявляет степень участия персонала в обработке защищаемой информации	ПК-3.2. 3-1. <b>Знает</b> содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации
		ПК-3.2. У-1. <b>Умеет</b> анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами
	ПК-3.3. Планирует мероприятия по обеспечению защиты информации в автоматизированной системе	ПК-3.3. 3-1. <b>Знает</b> организационные меры по защите информации
		ПК-3.3. У-1. <b>Умеет</b> организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению

		защищенных автоматизированных систем
ПК-3.4. Определяет требуемый класс (уровень) защищенности автоматизированной системы		ПК-3.4. 3-1. <b>Знает</b> руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
		ПК-3.4. У-1. <b>Умеет</b> классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации определять класс защищенности автоматизированных систем и ее составных частей
ПК-3.5. Обосновывает необходимость использования криптографических средств защиты информации		ПК-3.5. 3-1. <b>Знает</b> основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах
		ПК-3.5. У-1. <b>Умеет</b> обосновывать требования к системам защиты информации автоматизированных систем
ПК-3.6. Разрабатывает отчетные документы и разделы технических заданий		ПК-3.6. 3-1. <b>Знает</b> структуру и содержание основных разделов технических заданий на создание подсистем защиты информации автоматизированных систем
		ПК-3.6. У-1. <b>Умеет</b> разрабатывать технические задания на создание подсистем защиты информации автоматизированных систем

		и отчётные документы согласно требованиям проектной документации
ПК-4. Разработка эксплуатационной документации на системы защиты информации автоматизированных систем	ПК-4.1. Анализирует техническую документацию информационной инфраструктуры автоматизированной системы	ПК-4.1. 3-1. <b>Знает</b> руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
		ПК-4.1. У-1. <b>Умеет</b> разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем
	ПК-4.2. Анализирует защищенность информационной инфраструктуры автоматизированной системы	ПК-4.2. 3-1. <b>Знает</b> угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах
		ПК-4.2. У-1. <b>Умеет</b> исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных систем
	ПК-4.3. Формирует требования по защите информации, включая использование математического аппарата для решения прикладных задач	ПК-4.3. 3-1. <b>Знает</b> основные меры по защите информации в автоматизированных системах
		ПК-4.3. У-1. <b>Умеет</b> определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах
	ПК-4.4. Документирует программное	ПК-4.4. 3-1. <b>Знает</b> требования нормативных

	<p>обеспечение, технические средства, базы данных и компьютерные сети с учетом требований по обеспечению защиты информации</p>	<p>документов по обеспечению защиты информации</p>
	<p>ПК-4.5. Анализирует структурные и функциональные схемы защищенных автоматизированных информационных систем</p>	<p>ПК-4.4. У-1. <b>Умеет</b> документировать элементы информационных систем</p> <p>ПК-4.5. З-1. <b>Знает</b> методы построения и принципы функционирования современных автоматизированных систем</p> <p>ПК-4.5. У-1. <b>Умеет</b> определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем</p>
	<p>ПК-4.6. Обосновывает критерии эффективности функционирования защищенных автоматизированных информационных систем</p>	<p>ПК-4.6. З-1. <b>Знает</b> основные средства, способы и принципы построения систем защиты информации автоматизированных систем</p> <p>ПК-4.6. У-1. <b>Умеет</b> исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности</p>
	<p>ПК-4.7. Использует программно-аппаратные средства обеспечения безопасности информации в автоматизированных системах</p>	<p>ПК-4.7. З-1. <b>Знает</b> программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем</p> <p>ПК-4.7. У-1. <b>Умеет</b> анализировать программные,</p>

		архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем
ПК-5. Разработка архитектуры системы защиты информации автоматизированной системы	ПК-5.1. Проводит оценку показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации	ПК-5.1. 3-1. <b>Знает</b> основные информационные технологии, используемые в автоматизированных системах
		ПК-5.1. У-1. <b>Умеет</b> определять эффективность применения средств информатизации
	ПК-5.2. Проводит технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы	ПК-5.2. 3-1. <b>Знает</b> основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации
		ПК-5.2. У-1. <b>Умеет</b> разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем
	ПК-5.3. Определяет порядок обработки информации в автоматизированной системе	ПК-5.3. 3-1. <b>Знает</b> Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
		ПК-5.3. У-1. <b>Умеет</b> определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах

	ПК-5.4. Формирует разделы технических заданий на создание систем защиты информации автоматизированных систем	ПК-5.4. З-1. <b>Знает</b> национальные, межгосударственные и международные стандарты в области защиты информации
		ПК-5.4. У-1. <b>Умеет</b> определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите
	ПК-5.5. Разрабатывает проектную документацию на системы защиты автоматизированных систем	ПК-5.5. З-1. <b>Знает</b> основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации
		ПК-5.5. У-1. <b>Умеет</b> разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем
	ПК-5.6. Оформляет заявки на разработку систем защиты информации автоматизированных систем	ПК-5.6. З-1. <b>Знает</b> правила оформления заявок на разработку информационных систем
		ПК-5.6. У-1. <b>Умеет</b> обосновывать требования к системам защиты информации автоматизированных систем
ПК-6. Разработка проектных решений по защите информации в автоматизированных системах	ПК-6.1. Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах	ПК-6.1. З-1. <b>Знает</b> основные принципы моделирования
		ПК-6.1. У-1. <b>Умеет</b> выявлять основные угрозы безопасности информации и определять виды потенциальных нарушителей и их потенциалы
	ПК-6.2. Разрабатывает модели	ПК-6.2. З-1. <b>Знает</b> принципы построения и

	<p>автоматизированных систем и подсистем безопасности автоматизированных систем</p>	<p>функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов</p>
	<p>ПК-6.3. Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации</p>	<p>ПК-6.2. У-1. <b>Умеет</b> определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе</p> <p>ПК-6.3. З-1. <b>Знает</b> руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации</p> <p>ПК-6.3. У-1. <b>Умеет</b> применять действующую нормативную базу в области обеспечения защиты информации</p>
	<p>ПК-6.4. Разрабатывает предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах</p>	<p>ПК-6.4. З-1. <b>Знает</b> принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем</p> <p>ПК-6.4. У-1. <b>Умеет</b> определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в</p>

		области защиты информации автоматизированных систем
ПК-7. Определение угроз безопасности информации, обрабатываемой автоматизированной системой	ПК-7.1. Формирует разделы технических заданий на создание систем защиты информации автоматизированных систем	ПК-7.1. З-1. <b>Знает</b> принципы формирования и реализации политики безопасности информации в автоматизированных системах
		ПК-7.1. У-1. <b>Умеет</b> производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе
	ПК-7.2. Разрабатывает системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов	ПК-7.2. З-1. <b>Знает</b> национальные, межгосударственные и международные стандарты в области защиты информации
		ПК-7.2. У-1. <b>Умеет</b> формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы
	ПК-7.3. Определяет комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем	ПК-7.3. З-1. <b>Знает</b> способы реализации угроз безопасности в автоматизированных системах
		ПК-7.3. У-1. <b>Умеет</b> выявлять известные уязвимости информационных систем
	ПК-7.4. Определяет оценку возможностей внешних и внутренних нарушителей	ПК-7.4. З-1. <b>Знает</b> последствия от нарушения свойств безопасности информации

		ПК-7.4. У-1. <b>Умеет</b> анализировать возможные уязвимости информационных систем
ПК-7.5. Разрабатывает модели угроз безопасности информации автоматизированной системы		ПК-7.5. З-1. <b>Знает</b> принципы формирования и реализации политики безопасности информации в автоматизированных системах
		ПК-7.5. У-1. <b>Умеет</b> формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы
ПК-7.6. Обосновывает перечень сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы		ПК-7.6. З-1. <b>Знает</b> руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
		ПК-7.6. У-1. <b>Умеет</b> выбирать сертифицированные средства защиты информации в соответствии с требуемым уровнем защищённости
ПК-7.7. Анализирует требования к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации		ПК-7.7. З-1. <b>Знает</b> методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации
		ПК-7.7. У-1. <b>Умеет</b> систематизировать результаты проведенных исследований
ПК-7.8. Определяет структурно-функциональные		ПК-7.8. З-1. <b>Знает</b> программно-аппаратные средства обеспечения

	<p>характеристики информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации</p>	<p>защиты информации автоматизированных систем</p> <p>ПК-7.8. У-1. <b>Умеет</b> производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе</p>
<p>ПК-8. Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации</p>	<p>ПК-8.1. Разрабатывает аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем</p>	<p>ПК-8.1. З-1. <b>Знает</b> методы сбора и анализа научно-технической информации в области защиты информации</p> <p>ПК-8.1. У-1. <b>Умеет</b> извлекать необходимые знания в области защиты информации из имеющихся источников, в том числе, на иностранном языке и анализировать её</p>
	<p>ПК-8.2. Исследует аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем</p>	<p>ПК-8.2. З-1. <b>Знает</b> методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем</p>
		<p>ПК-8.2. У-1. <b>Умеет</b> выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации</p>
	<p>ПК-8.3. Разрабатывает модели угроз безопасности информации и нарушителей в автоматизированных системах</p>	<p>ПК-8.3. З-1. <b>Знает</b> основные способы применения математических моделей при проектировании систем защиты информации автоматизированных систем</p>
		<p>ПК-8.3. У-1. <b>Умеет</b> применять математические</p>

		модели при проектировании систем защиты информации автоматизированных систем
	ПК-8.4. Исследует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах	ПК-8.4. З-1. <b>Знает</b> основные меры по защите информации в автоматизированных системах
		ПК-8.4. У-1. <b>Умеет</b> выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации
	ПК-8.5. Анализирует информационную инфраструктуру и безопасность информации автоматизированных систем	ПК-8.5. З-1. <b>Знает</b> основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
		ПК-8.5. У-1. <b>Умеет</b> разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач
	ПК-8.6. Разрабатывает предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	ПК-8.6. З-1. <b>Знает</b> руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
		ПК-8.6. У-1. <b>Умеет</b> проектировать и реализовывать политику безопасности вычислительных сетей
ПК-9. Способен выбирать		ПК-9.1. З-1. <b>Знает</b> средства и методы хранения и передачи информации

технологии и основные компоненты обеспечивающей части создаваемых ИАС	ПК-9.1. Формирует функциональную часть ИАС	ПК-9.1. З-2. Знает нормативную базу, регламентирующую создание и эксплуатацию ИАС
		ПК-9.1. У-1. Умеет строить инфологическую модель предметной области
	ПК-9.2. Формирует технологию функционирования ИАС	ПК-9.2. З-1. Знает назначение и классификацию информационных и аналитических систем, систем управления
		ПК-9.2. У-1. Умеет выбирать эффективную технологию функционирования ИАС на базе моделирования
	ПК-9.3. Формирует конфигурацию и состав обеспечивающей части ИАС	ПК-9.3. З-1. Знает структуру функциональной и обеспечивающих частей ИАС
		ПК-9.3. З-2. Знает методы проектирования ИАС
		ПК-9.3. У-1. Умеет описывать функциональную часть ИАС ПК-9.3. У-2. Умеет производить сравнительный анализ вариантов конфигураций и состава обеспечивающей части ИАС
	ПК-9.4. Формирует комплекс мер защиты информации при создании ИАС	ПК-9.4. З-1. Знает принципы построения защищенных телекоммуникационных систем ПК-9.4. З-2. Знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации

		ПК-9.4. 3-3. Знает нормативные правовые акты в области защиты информации
		ПК-9.4. У-1. Умеет выбирать состав комплекса средств защиты информации в ИАС
ПК-10. Исследование эффективности ИАС	ПК-10.1. Формирует основные показатели и критерии эффективности ИАС	ПК-10.1. 3-1. Знает методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации
		ПК-10.1. 3-2. Знает критерии и показатели эффективности ИАС
		ПК-10.1. У-1. Умеет применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в ИАС
	ПК-10.2. Оценивает эффективность ИАС методами моделирования	ПК-10.2. 3-1. Знает методологические основы, методы и средства математического моделирования ИАС
ПК-10.2. 3-2. Знает методы теории вероятностей, теории случайных процессов и математической статистики		
		ПК-10.2. У-1. Умеет решать задачи исследования и оценки эффективности ИАС методами моделирования
		ПК-10.3. 3-1. Знает

	<p>ПК-10.3. Оценивает эффективность средств защиты информации в ИАС методами моделирования</p>	<p>основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации</p> <p>ПК-10.3. 3-2. Знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации</p> <p>ПК-10.3. У-1. <b>Умеет</b> классифицировать и оценивать угрозы информационной безопасности для объекта информатизации</p>
--	--	---

## 7. Структура и содержание практики (этапы формирования и критерии оценивания сформированности компетенций)

Общая трудоемкость проектно-технологической практики составляет 15 зачетных единиц, 540 часов.

Таблица 2

№	Разделы (этапы) практики	Виды работ, осуществляемых обучающимися	Трудоемкость (ак. час.)		Индикаторы достижения компетенций	Результаты обучения (знания, умения)	Формы текущего контроля
			Контакт т. работа	Сам.раб./практические. подготовка			
1	<b>Организационно-подготовительный</b>	<ul style="list-style-type: none"> <li>➤ вводное занятие/лекция;</li> <li>➤ инструктаж по технике безопасности;</li> <li>➤ инструктаж по подготовке отчета и процедуре защиты;</li> <li>➤ встреча с руководителями практики;</li> <li>➤ обсуждение и утверждение индивидуальных планов практикантов</li> </ul>	2	-	УК-1.1	УК-1.1. З-1.; УК-1.1. У-1.; УК-1.1. У-2	утверждение индивидуального задания по практике.
2	<b>Основной</b>	<ul style="list-style-type: none"> <li>➤ знакомство с базой практики/ изучение деятельности организации в целом и избранного структурного подразделения;</li> <li>➤ выполнение индивидуального задания;</li> <li>➤ сбор материалов для выполнения задания по</li> </ul>	2	514/514	УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-4.3; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ПК-1.1;	УК-1.1. З-1.; УК-1.1. У-1.; УК-1.1. У-2.; УК-1.2. У-1; УК-1.2. У-2.; УК-1.2. У-3.; УК-1.3. У-1.; УК-1.3. У-2.; УК-2.1. З-1.; УК-2.1-1. З-2.; УК-2.1. З-3.; УК-2.1. У-1.; УК-2.1. У-2.; УК-2.2. З-1.; УК-2.2. З-2.; УК-2.2. З-3.; УК-2.2. У-1.; УК-2.2. У-2.; УК-2.2. У-3.; УК-3.1. З-1.; УК-3.1. З-2.; УК-3.1. У-1.;	отчет/презентация части выполненного индивидуального задания.

		<p>практике/по теме выпускной работы;</p> <ul style="list-style-type: none"> <li>➤ анализ собранных материалов, проведение расчетов, составление графиков, диаграмм;</li> <li>➤ участие в решение конкретных профессиональных задач;</li> <li>➤ обработка и систематизация материала;</li> <li>➤ представление и обсуждение с руководителем проделанной части работы</li> </ul>			<p>ПК-1.2; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-2.5; ПК-2.6; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4; ПК-3.5; ПК-3.6; ПК-4.1; ПК-4.2; ПК-4.3; ПК-4.4; ПК-4.5; ПК-4.6; ПК-4.7; ПК-5.1; ПК-5.2; ПК-5.3; ПК-5.4; ПК-5.5; ПК-5.6; ПК-6.1; ПК-6.2; ПК-6.3; ПК-6.4; ПК-7.1; ПК-7.2; ПК-7.3; ПК-7.4; ПК-7.5; ПК-7.6; ПК-7.7; ПК-7.8; ПК-8.1; ПК-8.2; ПК-8.3; ПК-8.4; ПК-8.5; ПК-8.6; ПК-9.1; ПК-9.2; ПК-9.3; ПК-9.4; ПК-10.1; ПК-10.2; ПК-10.3</p>	<p>УК-3.1. У-2. УК-3.1. У-3.; УК-3.1. У-4.; УК-3.2. 3-1.; УК-3.2. 3-2.; УК-3.2. 3-3.; УК-3.2. У-1.; УК-3.2. У-2.; УК-3.2. У-3.; УК-3.2. У-4.; УК-4.1. 3-1.; УК-4.1. У-1.; УК-4.1. У-2.; УК-4.2. 3-1.; УК-4.2. У-1.; УК-4.3. У-1.; УК-4.3. У-2.; УК-5.1. 3-1.; УК-5.1. 3-2.; УК-5.1. 3-3.; УК-5.2. У-1.; УК-5.2. У-2.; УК-5.2. У-3.; УК-6.1. 3-1.; УК-6.1. 3-2.; УК-6.1. У-1.; УК-6.2. У-1.; УК-6.2. У-2.; ПК-1.1. 3-1.; ПК-1.1. У-1.; ПК-1.2. 3-1.; ПК-1.2. У-1.; ПК-2.1. 3-1.; ПК-2.1. У-1.; ПК-2.2. 3-1.; ПК-2.2. У-1.; ПК-2.3. 3-1.; ПК-2.3. У-1.; ПК-2.4. 3-1.; ПК-2.4. У-1.; ПК-2.5. 3-1.; ПК-2.5. У-1.; ПК-2.6. 3-1.; ПК-2.6. У-1.; ПК-3.1. 3-1.; ПК-3.1. У-1.; ПК-3.2. 3-1.; ПК-3.2. У-1.; ПК-3.3. 3-1.; ПК-3.3. У-1.; ПК-3.4. 3-1.; ПК-3.4. У-1.; ПК-3.5. 3-1.; ПК-3.5. У-1.; ПК-3.6. 3-1.; ПК-3.6. У-1.; ПК-4.1. 3-1.; ПК-4.1. У-1.; ПК-4.2. 3-1.; ПК-4.2. У-1.; ПК-4.3. 3-1.; ПК-4.3. У-1.; ПК-4.4. 3-1.; ПК-4.4. У-1.; ПК-4.5. 3-1.; ПК-4.5. У-1.; ПК-4.6. 3-1.; ПК-4.6. У-1.; ПК-4.7. 3-1.; ПК-4.7. У-1.; ПК-5.1. 3-1.; ПК-5.1. У-1.; ПК-5.2. 3-1.; ПК-5.2. У-1.; ПК-5.3. 3-1.; ПК-5.3. У-1.; ПК-5.4.</p>
--	--	---	--	--	--	---

						3-1.; ПК-5.4. У-1.; ПК-5.5. 3-1.; ПК-5.5. У-1.; ПК-5.6. 3-1.; ПК-5.6. У-1.; ПК-6.1. 3-1.; ПК-6.1. У-1.; ПК-6.2. 3-1.; ПК-6.2. У-1.; ПК-6.3. 3-1.; ПК-6.3. У-1.; ПК-6.4. 3-1.; ПК-6.4. У-1.; ПК-7.1. 3-1.; ПК-7.1. У-1.; ПК-7.2. 3-1.; ПК-7.2. У-1.; ПК-7.3. 3-1.; ПК-7.3. У-1.; ПК-7.4. 3-1.; ПК-7.4. У-1.; ПК-7.5. 3-1.; ПК-7.5. У-1.; ПК-7.6. 3-1.; ПК-7.6. У-1.; ПК-7.7. 3-1.; ПК-7.7. У-1.; ПК-7.8. 3-1.; ПК-7.8. У-1.; ПК-8.1. 3-1.; ПК-8.1. У-1.; ПК-8.2. 3-1.; ПК-8.2. У-1.; ПК-8.3. 3-1.; ПК-8.3. У-1.; ПК-8.4. 3-1.; ПК-8.4. У-1.; ПК-8.5. 3-1.; ПК-8.5. У-1.; ПК-8.6. 3-1.; ПК-8.6. У-1.; ПК-9.1. 3-1.; ПК-9.1. 3-2.; ПК-9.1. У-1.; ПК-9.2. 3-1.; ПК-9.2. У-1.; ПК-9.3. 3-1.; ПК-9.3. 3-2.; ПК-9.3. У-1.; ПК-9.3. У-2.; ПК-9.4. 3-1.; ПК-9.4. 3-2.; ПК-9.4. 3-3.; ПК-9.4. У-1.; ПК-10.1. 3-1.; ПК-10.1. 3-2.; ПК-10.1. У-1.; ПК-10.2. 3-1.; ПК-10.2. 3-2.; ПК-10.2. У-1.; ПК-10.3. 3-1.; ПК-10.3. 3-2.; ПК-10.3. У-1.	
3	<b>Отчетный</b>	➤ выработка на основе проведенного исследования выводов и предложений;	6	16/16	УК-4.1.	УК-4.1. 3-1.; УК-4.1. У-1.; УК-4.1. У-2.	Отчет по практике. Защита отчета.

		<ul style="list-style-type: none"> <li>➤ оформление результатов работы по практике в соответствии с установленными требованиями;</li> <li>➤ согласование отчета с руководителем практики, устранение замечаний;</li> <li>➤ сдача комплекта документов по практике на кафедру;</li> <li>➤ размещение документов в личном кабинете обучающегося;</li> <li>➤ защита отчета по практике с презентацией.</li> </ul>					
<b>Итого: 540 часов</b>			<b>10</b>	<b>530/530</b>			
<b><i>В том числе контактные часы на промежуточную аттестацию (зачет)</i></b>			<b>4</b>				

## **8. Образовательные, научно-исследовательские и научно-производственные технологии, используемые на практике**

В процессе прохождения практики используются следующие образовательные технологии:

- лекционные/практические занятия;
- самостоятельная работа студентов вне аудитории, в которую включается выполнение разделов практики в соответствии с индивидуальным заданием и рекомендованными источниками литературы;
- освоение методов анализа информации и интерпретации результатов;
- выполнение письменных аналитических и расчетных заданий в рамках практики с использованием необходимых информационных источников;
- консультации научного руководителя и руководителя практики от организации по актуальным вопросам, возникающим у студентов в ходе ее выполнения; методологии выполнения домашних заданий, подготовке отчета по практике и доклада по нему, выполнению аналитических заданий.
- обсуждение подготовленных обучающимися этапов работ по практике;
- сбор научной литературы по тематике индивидуального задания по практике;
- компьютерные технологии и программные продукты, используемые для сбора, систематизации, анализа информации;
- мультимедийные технологии для проведения ознакомительных мероприятий, презентации результатов исследований;
- защита отчета по практике с использованием презентаций;
- электронно-библиотечные системы для проведения научных исследований и аналитических разработок на основе изучения научной и учебно-методической литературы;
- справочно-правовые системы «Консультант +» и «Гарант»;

## **9. Учебно-методическое обеспечение самостоятельной работы обучающихся на практике**

Перечень образцов документов необходимых в процессе прохождения и защиты отчета по практике определяется следующими локальными нормативными актами:

- Положение о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования, федерального государственного бюджетного образовательного учреждения высшего образования «Российский экономический университет имени Г.В. Плеханова»;
- Регламент организации и проведения всех видов практик, обучающихся в Федеральном государственном бюджетном образовательном учреждении высшего образования «Российский экономический университет имени Г.В. Плеханова».

## **10. Формы отчетной документации и промежуточной аттестации**

**Формы отчетной документации** - комплект отчетных документов в соответствии с Регламентом организации и проведения практик, обучающихся в ФГОБУ ВО «РЭУ им. Г.В. Плеханова».

К защите отчета по практике допускаются обучающиеся, предоставившие полный комплект закрывающих практику документов.

Защита отчета проходит в последний день практики (с учетом календарного учебного графика по образовательной программе).

Отчеты по практике, выполненные на русском языке, подлежат проверке на объем неправомерных заимствований. Итоговая оценка оригинальности текста отчета по практике определяется в системе «Антиплагиат. ВУЗ» и закрепляется на уровне согласно указанному в Регламенте организации и проведения практик, обучающихся в ФГБОУ ВО «РЭУ им. Г.В. Плеханова».

Каждому обучающемуся необходимо в зависимости от тематики учебного задания, разработанного и выданного к выполнению руководителем практики и в соответствии с «Примерной тематикой учебных исследований в период проведения практики», выполнить индивидуальное задание, результаты которого разместить в отчете.

Структура отчета по практике должна включать разделы, отражающие выполнение заданий: общего задания и индивидуального задания.

Обучающиеся, не выполнившие программу практики без уважительной причины или получившие отрицательную оценку считаются имеющими академическую задолженность и обязаны ликвидировать академическую задолженность в порядке, установленном в локальных документах Университета.

**Промежуточная аттестация** осуществляется в соответствии с учебным планом во 2 семестре в форме зачета, который выставляется по результатам проверки отчетной документации, собеседования и защиты отчета с представлением презентации.

Промежуточная аттестация проводится при представлении обучающимся отчета по практике, включающего:

- титульный лист;
- индивидуальное задание;
- подготовленные в соответствии с индивидуальным заданием материалы;
- список использованной литературы.

## **11. Учебно-методическое и информационное обеспечение практики**

- Программа Технологической (проектно-технологической) практики;
- Положение о практической подготовке, утвержденное Приказом Министерства науки и высшего образования Российской Федерации и Министерством просвещения Российской Федерации от 05 августа 2020г. №885/390;
- Положение о практической подготовке обучающихся, осваивающих основные профессиональные образовательные программы высшего образования – программы бакалавриата, программы специалитета, программы магистратуры, программы подготовки научно-педагогических кадров в аспирантуре и осваивающих основные профессиональные образовательные программы среднего профессионального образования федерального государственного бюджетного образовательного учреждения высшего образования «Российский экономический университет имени Г.В. Плеханова»;
- Регламент организации и проведения практик, обучающихся, осваивающих основные профессиональные образовательные программы высшего образования- программы бакалавриата, программы специалитета, программы магистратуры ФГБОУ ВО «РЭУ имени Г.В. Плеханова».

### **Рекомендуемая литература**

#### **Основная литература:**

1. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. Ростов-на-Дону: Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1  
Режим доступа: <http://znanium.com/catalog/product/997105>
2. Инструментальные средства информационных систем: Учебное пособие / Вичугова А.А. Томск: Изд-во Томского политех. университета, 2015. - 136 с.: ISBN 978-5-4387-0574-1 Режим доступа: <http://znanium.com/catalog/product/673016>
3. Сбалансированно-целевое управление развитием предприятия: модели и технологии : монография / Б.Е. Одинцов ; под ред. проф. А.Н. Романова. — М. : Вузовский учебник : ИНФРА-М, 2018. — 162 с. — (Научная книга).  
Режим доступа: <http://znanium.com/catalog/product/937515>

#### **Дополнительная литература:**

1. Информационные технологии в науке и образовании : учеб. пособие / Е.Л. Федотова, А.А. Федотов. — Москва : ИД «ФОРУМ»; ИН-ФРА-М, 2015. — 336 с. — (Высшее образование). - ISBN 978-5-8199-0434-3 (ИД «ФОРУМ»); ISBN 978-5-16-004266-4 (ИНФРА-М, print); ISBN 978-5-16-103184-1 (ИНФРА-М, online)  
Режим доступа: <http://znanium.com/catalog/product/487293>
2. Баяндин, Н.И. Информационно-аналитическое обеспечение безопасности бизнеса. Деловая разведка: учебник / Н.И. Баяндин. - Санкт-Петербург: ИЦ "Интермедия", 2017. - 264 с.: схем., ил. - Библиогр. в кн. - ISBN 978-5-4383-0122-6;  
Режим доступа: <http://biblioclub.ru/index.php?page=book&id=482786>
3. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог: Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5  
Режим доступа: <http://znanium.com/catalog/product/997108>
4. Аппаратные и программные средства защиты информации: Учебное пособие / Душкин А.В., Кольцов А., Кравченко А. - Воронеж: Научная книга, 2016. - 232 с. ISBN 978-5-4446-0746-6  
Режим доступа: <http://znanium.com/catalog/product/923168>
5. Чернопятов, А.М. Бенчмаркинг: учебное пособие / А.М. Чернопятов. - Москва; Берлин: Директ-Медиа, 2018. - 154 с.: ил., табл. - Библиогр. в кн. - ISBN 978-5-4475-2760-0;  
Режим доступа: <http://biblioclub.ru/index.php?page=book&id=496622>

#### **Перечень справочно-библиографических изданий**

1. Ищейнов, В.Я. Информационная безопасность и защита информации: словарь терминов и понятий: словарь / Ищейнов В.Я. — Москва: Русайнс, 2019. — 226 с. — ISBN 978-5-4365-3184-7. — URL: <https://book.ru/book/932909>
2. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учеб. пособие / Ю. Н. Сычев, Рос. экон. ун-т им. Г.В. Плеханова. – М. : Изд-во РЭУ им. Г. В. Плеханова, 2017. – 206 с. : ил. – URL: [http://liber.rea.ru/action.php?kt\\_path\\_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1532](http://liber.rea.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1532) . – ISBN 978-5-7307-1148-8 : 162.15.

#### **Специализированная литература с грифом ДСП (ограниченного доступа):**

1. Актуальные вопросы информационной безопасности субъектов экономической деятельности: в 3 ч. – Ч. 1. Современные криптографические методы защиты информации: учебное пособие / А.В. Бабаш, В. В. Креопалов, А.А. Микрюков, В.А. Сизов. – Москва: ФГБОУ ВО «РЭУ им. Г.В. Плеханова», 2019. – 88 с. Инв. № 864

2. Актуальные вопросы информационной безопасности субъектов экономической деятельности: в 3 ч. – Ч. 2. Техническая защита информации: учебное пособие / А.В. Бабаш, В. В. Креопалов, А.А. Микрюков, В.А. Сизов. – Москва: ФГБОУ ВО «РЭУ им. Г.В. Плеханова», 2019. – 88 с. Инв. № 865
3. Актуальные вопросы информационной безопасности субъектов экономической деятельности: в 3 ч. – Ч. 3. Стандарты информационной безопасности сетей будущего: учебное пособие / А.В. Бабаш, В. В. Креопалов, А.А. Микрюков, В.А. Сизов. – Москва: ФГБОУ ВО «РЭУ им. Г.В. Плеханова», 2019. – 132 с. Инв. № 866

#### **Перечень специализированных отечественных и зарубежных периодических изданий**

##### **Отечественные периодические издания:**

1. Журнал «Информационная безопасность»
2. Журнал «Защита информации. Инсайд»

##### **Зарубежные периодические издания:**

3. Электронные ресурсы / Открытые зарубежные периодические издания по информационной безопасности / Журнал «Infosecurity Magazine»  
<https://www.infosecurity-magazine.com/>
4. Электронные ресурсы / Открытые зарубежные периодические издания по информационной безопасности / Журнал «(IN)SECURE Magazine»  
<https://www.helpnetsecurity.com/insecuremag-archive/>

#### **Перечень правовых нормативных актов и нормативных методических документов в области информационной безопасности**

1. Сизов В.А., Микрюков А.А., Креопалов В.В., Козырев П.А., Киров А.Д. Сборник нормативно-правовых документов в области информационной безопасности. М.: ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2019 – 364 с. – ISBN 978-5-7307-1618-6

#### **Перечень профессиональных баз данных**

1. Открытые профессиональные базы данных Федеральной службы по техническому и экспортному контролю - «Банк данных угроз» (<https://bdu.fstec.ru/threat> )
2. Открытые профессиональные базы данных Федеральной службы по техническому и экспортному контролю - «Список уязвимостей» ( <https://bdu.fstec.ru/vul> )

#### **Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины**

1. <http://www.fsb.ru/> (сайт ФСБ России);
2. <http://www.fstec.ru/> (сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России));
3. <http://www.komitet2-16.km.duma.gov.ru/> (сайт комитета Государственной Думы по безопасности);
4. <http://www.scrf.gov.ru/> (сайт Совета безопасности Российской Федерации);
5. <http://www.mvd.ru/> (сайт Министерства внутренних дел (МВД России)).

## **12. Материально-техническое обеспечение практики**

- Учебная аудитория для проведения учебных занятий лекционного /семинарского типа, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций, оснащенная оборудованием и техническими средствами обучения.
- Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с комплектом лицензионного программного обеспечения, с возможностью подключения к сети

«Интернет» и обеспечением доступа к электронной информационно-образовательной среде Университета.

- Библиотечный фонд ФГБОУ ВО «РЭУ им. Г.В. Плеханова».
- Материально-техническая база организации/предприятия, обеспечивающая проведение практики (практической подготовки), предусмотренной учебным планом и соответствующей действующим санитарным и противопожарным нормам и правилам.

### 13. Обязанности обучающегося при прохождении практики

Обязанности обучающегося при прохождении практики определяются Регламентом организации и проведения практик обучающихся, осваивающих основные профессиональные образовательные программы высшего образования, федерального государственного бюджетного образовательного учреждения высшего образования «Российский экономический университет имени Г.В. Плеханова».

### 14. Обязанности руководителя практики

Обязанности руководителя практики определяются Регламентом организации и проведения практик обучающихся, осваивающих основные профессиональные образовательные программы высшего образования, федерального государственного бюджетного образовательного учреждения высшего образования «Российский экономический университет имени Г.В. Плеханова».

### 15. Оценочные средства

Оценочные средства по практике разработаны в соответствии с Положением о фонде оценочных средств в ФГБОУ ВО «РЭУ им. Г.В. Плеханова».

**Перечень планируемых результатов обучения при прохождении практики, соотнесенных с требуемыми индикаторами достижения компетенций и компетенциями выпускников – указаны в таблице 1, раздел 6.**

**Этапы формирования и критерии оценивания сформированности компетенций - указаны в таблице 2, раздел 7.**

Предметом оценки по практике является приобретение практического опыта. Контроль и оценка по практике проводится на основе индивидуального задания обучающегося с указанием конкретных видов работ, их объема, качества выполнения в соответствии с технологией и требованиями образовательного учреждения; отзыва руководителя по практике; отчета по практике.

**Типовые задания и иные материалы, необходимые для оценки знаний, умений, характеризующих этапы формирования компетенций в процессе прохождения практики указаны в Приложении 1.**

В процессе прохождения практики руководителем по практике контролируется формирование у обучающихся соответствующих компетенций и ее составляющих.

**Виды оценочных средств, используемых для оценки сформированности компетенций**

*Таблица 3*

Формируемые компетенции	Индикаторы достижения компетенций	Виды оценочных средств		
		Выполнение индивидуального задания	Отчет по практике	Защита отчета по практике
УК-1. Способен осуществлять	УК-1.1. Анализирует проблемную ситуацию как	+	+	+

критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	целостную систему, выявляя ее составляющие и связи между ними УК-1.2. Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации УК-1.3. Вырабатывает стратегию действий для решения проблемной ситуации в виде последовательности шагов, предвидя результат каждого из них			
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Понимает принципы проектного подхода к управлению УК-2.2. Демонстрирует способность управления проектами	+	+	+
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1. Понимает и знает особенности формирования эффективной команды УК-3.2. Демонстрирует поведение эффективного организатора и координатора командного взаимодействия	+	+	+
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Составляет в соответствии с нормами государственного языка РФ и иностранного языка документы (письма, эссе, рефераты и др.) для академического и профессионального взаимодействия УК-4.2. Представляет результаты академической и профессиональной деятельности на мероприятиях различного формата, включая международные УК-4.3. Принимает участие в академических и профессиональных дискуссиях, в том числе на иностранном(ых) языке(ах)	+	+	+
УК-5. Способен анализировать и	УК-5.1. Имеет представление о сущности и принципах анализа	+	+	+

учитывать разнообразие культур в процессе межкультурного взаимодействия	разнообразия культур в процессе межкультурного взаимодействия УК-5.2. Демонстрирует способность анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия			
УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1. Определяет стимулы, мотивы и приоритеты собственной профессиональной деятельности и цели карьерного роста УК-6.2. Проводит рефлексию своей деятельности и разрабатывает способы ее совершенствования	+	+	+
ПК-1. Обеспечение информационной безопасности вычислительных сетей	ПК-1.1. Анализирует основные характеристики и возможности телекоммуникационных систем по передаче информации ПК-1.2. Проектирует и реализует политику безопасности вычислительных сетей	+	+	+
ПК-2. Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	ПК-2.1. Разрабатывает техническую документацию в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем ПК-2.2. Применяет средства схемотехнического проектирования и современную измерительную аппаратуру ПК-2.3. Синтезирует структурные и функциональные схемы защищенных автоматизированных систем ПК-2.4. Разрабатывает программное обеспечение,	+	+	+

	<p>технические средства, базы данных и компьютерные сети с учетом требований по обеспечению защиты информации</p> <p>ПК-2.5. Разрабатывает электронные схемы с учетом требований по защите информации автоматизированных и информационных систем</p> <p>ПК-2.6. Оптимизирует работу электронных схем с учетом требований по защите информации</p>			
<p>ПК-3. Обоснование необходимости защиты информации в автоматизированной системе</p>	<p>ПК-3.1. Анализирует характер обрабатываемой информации и определяет перечень информации, подлежащей защите</p> <p>ПК-3.2. Выявляет степень участия персонала в обработке защищаемой информации</p> <p>ПК-3.3. Планирует мероприятия по обеспечению защиты информации в автоматизированной системе</p> <p>ПК-3.4. Определяет требуемый класс (уровень) защищенности автоматизированной системы</p> <p>ПК-3.5. Обосновывает необходимость использования криптографических средств защиты информации</p> <p>ПК-3.6. Разрабатывает отчетные документы и разделы технических заданий</p>	<p style="text-align: center;">+</p>	<p style="text-align: center;">+</p>	<p style="text-align: center;">+</p>
<p>ПК-4. Разработка эксплуатационной документации на системы защиты информации автоматизированных систем</p>	<p>ПК-4.1. Анализирует техническую документацию информационной инфраструктуры автоматизированной системы</p> <p>ПК-4.2. Анализирует защищенность информационной инфраструктуры автоматизированной системы</p> <p>ПК-4.3. Формирует требования по защите информации,</p>	<p style="text-align: center;">+</p>	<p style="text-align: center;">+</p>	<p style="text-align: center;">+</p>

	<p>включая использование математического аппарата для решения прикладных задач</p> <p>ПК-4.4. Документирует программное обеспечение, технические средства, базы данных и компьютерные сети с учетом требований по обеспечению защиты информации</p> <p>ПК-4.5. Анализирует структурные и функциональные схемы защищенных автоматизированных информационных систем</p> <p>ПК-4.6. Обосновывает критерии эффективности функционирования защищенных автоматизированных информационных систем</p> <p>ПК-4.7. Использует программно-аппаратные средства обеспечения безопасности информации в автоматизированных системах</p>			
<p>ПК-5. Разработка архитектуры системы защиты информации автоматизированной системы</p>	<p>ПК-5.1. Проводит оценку показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации</p> <p>ПК-5.2. Проводит технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы</p> <p>ПК-5.3. Определяет порядок обработки информации в автоматизированной системе</p> <p>ПК-5.4. Формирует разделы технических заданий на создание систем защиты информации автоматизированных систем</p>	<p style="text-align: center;">+</p>	<p style="text-align: center;">+</p>	<p style="text-align: center;">+</p>

	<p>ПК-5.5. Разрабатывает проектную документацию на системы защиты автоматизированных систем</p> <p>ПК-5.6. Оформляет заявки на разработку систем защиты информации автоматизированных систем</p>			
<p>ПК-6. Разработка проектных решений по защите информации в автоматизированных системах</p>	<p>ПК-6.1. Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах</p> <p>ПК-6.2. Разрабатывает модели автоматизированных систем и подсистем безопасности автоматизированных систем</p> <p>ПК-6.3. Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации</p> <p>ПК-6.4. Разрабатывает предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах</p>	+	+	+
<p>ПК-7. Определение угроз безопасности информации, обрабатываемой автоматизированной системой</p>	<p>ПК-7.1. Формирует разделы технических заданий на создание систем защиты информации автоматизированных систем</p> <p>ПК-7.2. Разрабатывает системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов</p> <p>ПК-7.3. Определяет комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем</p> <p>ПК-7.4. Определяет оценку возможностей внешних и внутренних нарушителей</p>	+	+	+

	<p>ПК-7.5. Разрабатывает модели угроз безопасности информации автоматизированной системы</p> <p>ПК-7.6. Обосновывает перечень сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы</p> <p>ПК-7.7. Анализирует требования к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации</p> <p>ПК-7.8. Определяет структурно-функциональные характеристики информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации</p>			
<p>ПК-8. Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации</p>	<p>ПК-8.1. Разрабатывает аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем</p> <p>ПК-8.2. Исследует аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем</p> <p>ПК-8.3. Разрабатывает модели угроз безопасности информации и нарушителей в автоматизированных системах</p> <p>ПК-8.4. Исследует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей</p>	<p style="text-align: center;">+</p>	<p style="text-align: center;">+</p>	<p style="text-align: center;">+</p>

	<p>безопасности информации в автоматизированных системах</p> <p>ПК-8.5. Анализирует информационную инфраструктуру и безопасность информации автоматизированных систем</p> <p>ПК-8.6. Разрабатывает предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем</p>			
<p>ПК-9. Способен выбирать технологии и основные компоненты обеспечивающей части создаваемых ИАС</p>	<p>ПК-9.1. Формирует функциональную часть ИАС</p> <p>ПК-9.2. Формирует технологию функционирования ИАС</p> <p>ПК-9.3. Формирует конфигурацию и состав обеспечивающей части ИАС</p> <p>ПК-9.4. Формирует комплекс мер защиты информации при создании ИАС</p>	+	+	+
<p>ПК-10. Исследование эффективности ИАС</p>	<p>ПК-10.1. Формирует основные показатели и критерии эффективности ИАС</p> <p>ПК-10.2. Оценивает эффективность ИАС методами моделирования</p> <p>ПК-10.3. Оценивает эффективность средств защиты информации в ИАС методами моделирования</p>	+	+	+

**Форма отзыва руководителя по практике с указанием баллов** оформляются в соответствии с Регламентом организации и проведения практик обучающихся, осваивающих основные профессиональные образовательные программы высшего образования, федерального государственного бюджетного образовательного учреждения высшего образования «Российский экономический университет имени Г.В. Плеханова».

**Показатели и критерии оценивания планируемых результатов освоения компетенций и результатов обучения,  
шкала оценивания**

Таблица 4

Шкала оценивания		Формируемые компетенции	Индикатор достижения компетенции	Критерии оценивания	Уровень освоения компетенций
85 – 100 баллов	«отлично»/ «зачтено»	УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10.	УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-4.3; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ПК-1.1; ПК-1.2; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-2.5; ПК-2.6; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4; ПК-3.5; ПК-3.6; ПК-4.1; ПК-4.2; ПК-4.3; ПК-4.4; ПК-4.5; ПК-4.6; ПК-4.7; ПК-5.1; ПК-5.2; ПК-5.3; ПК-5.4; ПК-5.5; ПК-5.6; ПК-6.1;	<p><b>Знает верно и в полном объеме:</b> методику постановки цели и определения способов ее достижения; основные методологические подходы в сфере управления проектами; методы и модели структуризации проекта; методы управления рисками проекта на всех стадиях его жизненного цикла; основные виды проектов их специфику и особенности управления ими; способы оценки проектов с учетом факторов риска и неопределенности; основные принципы управления проектами на всех стадиях жизненного цикла; основные модели командообразования и факторы, влияющие на эффективность командной работы; основные современные технологии организации деятельности команд, в том числе – виртуальных; основные методы анализа взаимодействия в команде; основные современные технологии коммуникации различного типа; принципы предоставления обратной связи; методы и способы применения информационно-коммуникационных технологий для сбора, хранения, обработки, представления и передачи информации в ситуациях академического и профессионального взаимодействия; основные концепции организации межличностного взаимодействия в информационной среде; принципы анализа и учета разнообразия культур в процессе межкультурного взаимодействия; методы анализа и учета разнообразия культур в процессе межкультурного взаимодействия; нормы межкультурного взаимодействия с учетом разнообразия культур; основные принципы мотивации и стимулирования карьерного развития; способы самооценки и самоопределения;</p> <p>основные типы и характеристики сетевого оборудования отечественных и ведущих мировых производителей; основные методологии проектирования политик информационной безопасности вычислительных сетей; нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных</p>	Продвинутый

			<p>ПК-6.2; ПК-6.3; ПК-6.4; ПК-7.1; ПК-7.2; ПК-7.3; ПК-7.4; ПК-7.5; ПК-7.6; ПК-7.7; ПК-7.8; ПК-8.1; ПК-8.2; ПК-8.3; ПК-8.4; ПК-8.5; ПК-8.6; ПК-9.1; ПК-9.2; ПК-9.3; ПК-9.4; ПК-10.1; ПК-10.2; ПК-10.3.</p>	<p>федеральных органов исполнительной власти по защите информации; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схмотехнические решения основных узлов и блоков электронной аппаратуры; основные информационные технологии, используемые в автоматизированных системах; современные технологии программирования, особенности защиты информации в автоматизированных системах управления технологическими процессами; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схмотехнические решения основных узлов и блоков электронной аппаратуры; методы оптимизации схмотехнических решений; виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; организационные меры по защите информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах; структуру и содержание основных разделов технических заданий на создание подсистем защиты информации автоматизированных систем; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах; основные меры по защите информации в автоматизированных системах; требования нормативных документов по обеспечению защиты информации; методы построения и принципы функционирования современных автоматизированных систем; основные средства, способы и принципы построения систем защиты информации автоматизированных систем; программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем; основные информационные технологии, используемые в автоматизированных системах; основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; руководящие и методические документы</p>	
--	--	--	---	---	--

			<p>уполномоченных федеральных органов исполнительной власти по защите информации; национальные, межгосударственные и международные стандарты в области защиты информации; основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; правила оформления заявок на разработку информационных систем; основные принципы моделирования; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем; принципы формирования и реализации политики безопасности информации в автоматизированных системах; национальные, межгосударственные и международные стандарты в области защиты информации; способы реализации угроз безопасности в автоматизированных системах; последствия от нарушения свойств безопасности информации; принципы формирования и реализации политики безопасности информации в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации; программно-аппаратные средства обеспечения защиты информации автоматизированных систем; методы сбора и анализа научно-технической информации в области защиты информации; методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем; основные способы применения математических моделей при проектировании систем защиты информации автоматизированных систем; основные меры по защите информации в автоматизированных системах; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;</p>	
--	--	--	---	--

			<p>средства и методы хранения и передачи информации; нормативную базу, регламентирующую создание и эксплуатацию ИАС; назначение и классификацию информационных и аналитических систем, систем управления; структуру функциональной и обеспечивающих частей ИАС; методы проектирования ИАС; принципы построения защищенных телекоммуникационных систем; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; нормативные правовые акты в области защиты информации; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; критерии и показатели эффективности ИАС; методологические основы, методы и средства математического моделирования ИАС; методы теории вероятностей, теории случайных процессов и математической статистики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.</p> <p><b>Умеет верно и в полном объеме:</b></p> <p>определить суть проблемной ситуации и этапы ее разрешения с учетом вариативных контекстов; осуществлять сбор, систематизацию и критический анализ информации, необходимой для выработки стратегии действий по разрешению проблемной ситуации; проводит оценку адекватности и достоверности информации о проблемной ситуации, умеет работать с противоречивой информацией из разных источников; осуществляет поиск решений проблемной ситуации на основе действий, эксперимента и опыта; критически оценивает возможные варианты решения проблемной ситуации на основе анализа причинно-следственных связей; осуществляет и аргументирует выбор стратегии по решению проблемной ситуации, оценивает преимущества и недостатки выбранной стратегии; осуществляет разработку плана действий по решению проблемной ситуации, определяет и оценивает практические последствия реализации действий по разрешению проблемной ситуации; строить и структурировать жизненный цикл проекта; применяет основные процедуры и методы управления проектами и подготовки проектных решений; планировать реализацию проекта; оценивать эффективности проектов; измерять и анализировать результаты проектной деятельности;</p>	
--	--	--	---	--

			<p>определять роль каждого участника команды; ставить перед каждым участником команды четко сформулированную задачу с учетом его роли; выбирать методы организации работы команды с учетом специфики поставленной цели, временных и прочих ограничений; составлять планы и графики основных шагов по достижению поставленной перед командой цели и оценивать необходимые временные, информационные и другие ресурсы; поддерживать в команде атмосферу сотрудничества и достижения цели, показывая ценность вклада каждого участника; предоставлять эффективную обратную связь участникам команды по промежуточным и конечным результатам работы; выявлять конфликты, возникающие в процессе командной работы, и конструктивно управлять ими; использовать различные типы коммуникации для обеспечения эффективного взаимодействия участников команды, в том числе – виртуальной; самостоятельно находит и обрабатывает информацию, необходимую для качественного выполнения академических и профессиональных задач и достижения профессионально значимых целей, в т.ч. на иностранном языке; составляет, редактирует на государственном языке РФ и/или иностранном языке, выполняет корректный перевод с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный язык различных академических и профессиональных текстов; владеет навыками и умениями установления и развития академических и профессиональных контактов, в т.ч. в международной среде, в соответствии с целями, задачами и условиями совместной деятельности, включая обмен информацией и выработку единой стратегии взаимодействия; воспринимает и анализирует информацию на государственном языке РФ и иностранном языке в процессе академического и профессионального взаимодействия; принимает участие в академических и профессиональных дискуссиях на государственном языке РФ и/или иностранном языке, аргументированно отстаивая свои позиции и идеи; анализировать разнообразие культур в процессе межкультурного взаимодействия; учитывать разнообразие культур в процессе межкультурного взаимодействия; строить межкультурное взаимодействие с учетом разнообразия культур; оценить возможности реализации собственных профессиональных целей и расставить приоритеты; провести анализ результатов своей социальной и</p>	
--	--	--	---	--

			<p>профессиональной деятельности; корректировать планы личного и профессионального развития;</p> <p>осуществлять подбор сетевого оборудования для конкретных организаций и эксплуатировать сетевое оборудование; разрабатывать и реализовывать политики работы в корпоративных сетях, проектировать и эксплуатировать локальные вычислительные сети, восстанавливать их работоспособность; разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД; проводить комплексное тестирование аппаратных и программных средств; оценивать сложность алгоритмов и вычислений; разрабатывать программное обеспечение, технические средства, базы данных и компьютерные сети с учетом требований по обеспечению защиты информации; осуществлять мониторинг и оперативное устранение уязвимостей в программном и аппаратном обеспечении, выявлять уязвимости в программном и аппаратном обеспечении; оценивать сложность алгоритмов и вычислений; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации; анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами; организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации; определять класс защищенности автоматизированных систем и ее составных частей; обосновывать требования к системам защиты информации автоматизированных систем; разрабатывать технические задания на создание подсистем защиты информации автоматизированных систем и отчетные документы согласно требованиям проектной документации; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем; исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных систем; определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах; документировать элементы информационных систем; определять</p>	
--	--	--	--	--

			<p>структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем; исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности; анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем; определять эффективность применения средств информатизации; разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах; определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите; разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; обосновывать требования к системам защиты информации автоматизированных систем; выявлять основные угрозы безопасности информации и определять виды потенциальных нарушителей и их потенциалы; определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе; применять действующую нормативную базу в области обеспечения защиты информации; определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем; производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе; формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы; выявлять известные уязвимости информационных систем; анализировать возможные уязвимости информационных систем; формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы; выбирать сертифицированные средства</p>	
--	--	--	--	--

				защиты информации в соответствии с требуемым уровнем защищённости; систематизировать результаты проведенных исследований; производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе; извлекать необходимые знания в области защиты информации из имеющихся источников, в том числе, на иностранном языке и анализировать её; выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации; применять математические модели при проектировании систем защиты информации автоматизированных систем; выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации; разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач; проектировать и реализовывать политику безопасности вычислительных сетей; строить инфологическую модель предметной области; выбирать эффективную технологию функционирования ИАС на базе моделирования; описывать функциональную часть ИАС; производить сравнительный анализ вариантов конфигураций и состава обеспечивающей части ИАС; выбирать состав комплекса средств защиты информации в ИАС; применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в ИАС; решать задачи исследования и оценки эффективности ИАС методами моделирования; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.	
<b>70 – 84 баллов</b>	<b>«хорошо»/ «зачтено»</b>	УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10.	УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-4.3; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ПК-1.1;	<b>Знает с незначительными замечаниями:</b> методику постановки цели и определения способов ее достижения; основные методологические подходы в сфере управления проектами; методы и модели структуризации проекта; методы управления рисками проекта на всех стадиях его жизненного цикла; основные виды проектов их специфику и особенности управления ими; способы оценки проектов с учетом факторов риска и неопределенности; основные принципы управления проектами на всех стадиях жизненного цикла; основные модели командообразования и факторы, влияющие на эффективность командной работы; основные модели командообразования и факторы, влияющие на эффективность командной работы; основные современные	<b>Повышенный</b>

			<p>ПК-1.2; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-2.5; ПК-2.6; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4; ПК-3.5; ПК-3.6; ПК-4.1; ПК-4.2; ПК-4.3; ПК-4.4; ПК-4.5; ПК-4.6; ПК-4.7; ПК-5.1; ПК-5.2; ПК-5.3; ПК-5.4; ПК-5.5; ПК-5.6; ПК-6.1; ПК-6.2; ПК-6.3; ПК-6.4; ПК-7.1; ПК-7.2; ПК-7.3; ПК-7.4; ПК-7.5; ПК-7.6; ПК-7.7; ПК-7.8; ПК-8.1; ПК-8.2; ПК-8.3; ПК-8.4; ПК-8.5; ПК-8.6; ПК-9.1; ПК-9.2; ПК-9.3; ПК-9.4; ПК-10.1; ПК-</p>	<p>технологии организации деятельности команд, в том числе – виртуальных; основные методы анализа взаимодействия в команде; основные современные технологии коммуникации различного типа; принципы предоставления обратной связи; методы и способы применения информационно-коммуникационных технологий для сбора, хранения, обработки, представления и передачи информации в ситуациях академического и профессионального взаимодействия; основные концепции организации межличностного взаимодействия в информационной среде; принципы анализа и учета разнообразия культур в процессе межкультурного взаимодействия; методы анализа и учета разнообразия культур в процессе межкультурного взаимодействия; нормы межкультурного взаимодействия с учетом разнообразия культур; основные принципы мотивации и стимулирования карьерного развития; способы самооценки и самоопределения;</p> <p>основные типы и характеристики сетевого оборудования отечественных и ведущих мировых производителей; основные методологии проектирования политик информационной безопасности вычислительных сетей; нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; основные информационные технологии, используемые в автоматизированных системах; современные технологии программирования, особенности защиты информации в автоматизированных системах управления технологическими процессами; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; методы оптимизации схемотехнических решений; виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; организационные меры по защите информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; основные</p>	
--	--	--	---	---	--

			10.2; ПК-10.3.	криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах; структуру и содержание основных разделов технических заданий на создание подсистем защиты информации автоматизированных систем; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах; основные меры по защите информации в автоматизированных системах; требования нормативных документов по обеспечению защиты информации; методы построения и принципы функционирования современных автоматизированных систем; основные средства, способы и принципы построения систем защиты информации автоматизированных систем; программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем; основные информационные технологии, используемые в автоматизированных системах; основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; национальные, межгосударственные и международные стандарты в области защиты информации; основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; правила оформления заявок на разработку информационных систем; основные принципы моделирования; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем; принципы формирования и реализации политики безопасности информации в автоматизированных системах; национальные, межгосударственные и международные стандарты в области защиты информации; способы	
--	--	--	----------------	--	--

			<p>реализации угроз безопасности в автоматизированных системах; последствия от нарушения свойств безопасности информации; принципы формирования и реализации политики безопасности информации в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации; программно-аппаратные средства обеспечения защиты информации автоматизированных систем; методы сбора и анализа научно-технической информации в области защиты информации; методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем; основные способы применения математических моделей при проектировании систем защиты информации автоматизированных систем; основные меры по защите информации в автоматизированных системах; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; средства и методы хранения и передачи информации; нормативную базу, регламентирующую создание и эксплуатацию ИАС; назначение и классификацию информационных и аналитических систем, систем управления; структуру функциональной и обеспечивающих частей ИАС; методы проектирования ИАС; принципы построения защищенных телекоммуникационных систем; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; нормативные правовые акты в области защиты информации; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; критерии и показатели эффективности ИАС; методологические основы, методы и средства математического моделирования ИАС; методы теории вероятностей, теории случайных процессов и математической статистики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.</p>	
--	--	--	--	--

			<p><b>Умеет с незначительными замечаниями:</b> определить суть проблемной ситуации и этапы ее разрешения с учетом вариативных контекстов; осуществлять сбор, систематизацию и критический анализ информации, необходимой для выработки стратегии действий по разрешению проблемной ситуации; проводит оценку адекватности и достоверности информации о проблемной ситуации, умеет работать с противоречивой информацией из разных источников; осуществляет поиск решений проблемной ситуации на основе действий, эксперимента и опыта; критически оценивает возможные варианты решения проблемной ситуации на основе анализа причинно-следственных связей; осуществляет и аргументирует выбор стратегии по решению проблемной ситуации, оценивает преимущества и недостатки выбранной стратегии; осуществляет разработку плана действий по решению проблемной ситуации, определяет и оценивает практические последствия реализации действий по разрешению проблемной ситуации; строить и структурировать жизненный цикл проекта; применяет основные процедуры и методы управления проектами и подготовки проектных решений; планировать реализацию проекта; оценивать эффективности проектов; измерять и анализировать результаты проектной деятельности; определять роль каждого участника команды; ставить перед каждым участником команды четко сформулированную задачу с учетом его роли; выбирать методы организации работы команды с учетом специфики поставленной цели, временных и прочих ограничений; составлять планы и графики основных шагов по достижению поставленной перед командой цели и оценивать необходимые временные, информационные и другие ресурсы; поддерживать в команде атмосферу сотрудничества и достижения цели, показывая ценность вклада каждого участника; предоставлять эффективную обратную связь участникам команды по промежуточным и конечным результатам работы; выявлять конфликты, возникающие в процессе командной работы, и конструктивно управлять ими; использовать различные типы коммуникации для обеспечения эффективного взаимодействия участников команды, в том числе – виртуальной; самостоятельно находит и обрабатывает информацию, необходимую для качественного выполнения академических и профессиональных задач и достижения профессионально значимых целей, в т.ч. на иностранном языке; составляет, редактирует на государственном языке РФ и/или иностранном языке, выполняет</p>	
--	--	--	--	--

			<p>корректный перевод с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный язык различных академических и профессиональных текстов; владеет навыками и умениями установления и развития академических и профессиональных контактов, в т.ч. в международной среде, в соответствии с целями, задачами и условиями совместной деятельности, включая обмен информацией и выработку единой стратегии взаимодействия; воспринимает и анализирует информацию на государственном языке РФ и иностранном языке в процессе академического и профессионального взаимодействия; принимает участие в академических и профессиональных дискуссиях на государственном языке РФ и/или иностранном языке, аргументированно отстаивая свои позиции и идеи; анализировать разнообразие культур в процессе межкультурного взаимодействия; учитывать разнообразие культур в процессе межкультурного взаимодействия; строить межкультурное взаимодействие с учетом разнообразия культур; оценить возможности реализации собственных профессиональных целей и расставить приоритеты; провести анализ результатов своей социальной и профессиональной деятельности; корректировать планы личного и профессионального развития;</p> <p>осуществлять подбор сетевого оборудования для конкретных организаций и эксплуатировать сетевое оборудование; разрабатывать и реализовывать политики работы в корпоративных сетях, проектировать и эксплуатировать локальные вычислительные сети, восстанавливать их работоспособность; разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД; проводить комплексное тестирование аппаратных и программных средств; оценивать сложность алгоритмов и вычислений; разрабатывать программное обеспечение, технические средства, базы данных и компьютерные сети с учетом требований по обеспечению защиты информации; осуществлять мониторинг и оперативное устранение уязвимостей в программном и аппаратном обеспечении, выявлять уязвимости в программном и аппаратном обеспечении; оценивать сложность алгоритмов и вычислений; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности</p>	
--	--	--	--	--

			<p>информации; анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами; организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации определять класс защищенности автоматизированных систем и ее составных частей; обосновывать требования к системам защиты информации автоматизированных систем; разрабатывать технические задания на создание подсистем защиты информации автоматизированных систем и отчетные документы согласно требованиям проектной документации; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем; исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных систем; определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах; документировать элементы информационных систем; определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем; исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности; анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем; определять эффективность применения средств информатизации; разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах; определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите; разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем;</p>	
--	--	--	---	--

			<p>обосновывать требования к системам защиты информации автоматизированных систем; выявлять основные угрозы безопасности информации и определять виды потенциальных нарушителей и их потенциалы; определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе; применять действующую нормативную базу в области обеспечения защиты информации; определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем; производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе; формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы; выявлять известные уязвимости информационных систем; анализировать возможные уязвимости информационных систем; формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы; выбирать сертифицированные средства защиты информации в соответствии с требуемым уровнем защищенности; систематизировать результаты проведенных исследований; производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе; извлекать необходимые знания в области защиты информации из имеющихся источников, в том числе, на иностранном языке и анализировать её; выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации; применять математические модели при проектировании систем защиты информации автоматизированных систем; выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации; разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач; проектировать и реализовывать политику безопасности вычислительных сетей; строить инфологическую модель</p>	
--	--	--	---	--

				<p>предметной области; выбирать эффективную технологию функционирования ИАС на базе моделирования; описывать функциональную часть ИАС; производить сравнительный анализ вариантов конфигураций и состава обеспечивающей части ИАС; выбирать состав комплекса средств защиты информации в ИАС; применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в ИАС; решать задачи исследования и оценки эффективности ИАС методами моделирования; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.</p>	
<p><b>50 – 69 баллов</b></p>	<p>«удовлетворительно»/ «зачтено»</p>	<p>УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10.</p>	<p>УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-4.3; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ПК-1.1; ПК-1.2; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-2.5; ПК-2.6; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4; ПК-3.5; ПК-3.6; ПК-4.1; ПК-4.2; ПК-4.3; ПК-4.4; ПК-4.5; ПК-4.6; ПК-4.7; ПК-5.1;</p>	<p><b>Знает на базовом уровне, с ошибками:</b> методику постановки цели и определения способов ее достижения; основные методологические подходы в сфере управления проектами; методы и модели структуризации проекта; методы управления рисками проекта на всех стадиях его жизненного цикла; основные виды проектов их специфику и особенности управления ими; способы оценки проектов с учетом факторов риска и неопределенности; основные принципы управления проектами на всех стадиях жизненного цикла; основные модели командообразования и факторы, влияющие на эффективность командной работы; основные модели командообразования и факторы, влияющие на эффективность командной работы; основные современные технологии организации деятельности команд, в том числе – виртуальных; основные методы анализа взаимодействия в команде; основные современные технологии коммуникации различного типа; принципы предоставления обратной связи; методы и способы применения информационно-коммуникационных технологий для сбора, хранения, обработки, представления и передачи информации в ситуациях академического и профессионального взаимодействия; основные концепции организации межличностного взаимодействия в информационной среде; принципы анализа и учета разнообразия культур в процессе межкультурного взаимодействия; методы анализа и учета разнообразия культур в процессе межкультурного взаимодействия; нормы межкультурного взаимодействия с учетом разнообразия культур; основные принципы мотивации и стимулирования карьерного развития; способы самооценки и самоопределения;</p>	<p><b>Базовый</b></p>

			<p>ПК-5.2; ПК-5.3; ПК-5.4; ПК-5.5; ПК-5.6; ПК-6.1; ПК-6.2; ПК-6.3; ПК-6.4; ПК-7.1; ПК-7.2; ПК-7.3; ПК-7.4; ПК-7.5; ПК-7.6; ПК-7.7; ПК-7.8; ПК-8.1; ПК-8.2; ПК-8.3; ПК-8.4; ПК-8.5; ПК-8.6; ПК-9.1; ПК-9.2; ПК-9.3; ПК-9.4; ПК-10.1; ПК-10.2; ПК-10.3.</p>	<p>основные типы и характеристики сетевого оборудования отечественных и ведущих мировых производителей; основные методологии проектирования политик информационной безопасности вычислительных сетей; нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; основные информационные технологии, используемые в автоматизированных системах; современные технологии программирования, особенности защиты информации в автоматизированных системах управления технологическими процессами; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; методы оптимизации схемотехнических решений; виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; организационные меры по защите информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах; структуру и содержание основных разделов технических заданий на создание подсистем защиты информации автоматизированных систем; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах; основные меры по защите информации в автоматизированных системах; требования нормативных документов по обеспечению защиты информации; методы построения и принципы функционирования современных автоматизированных систем; основные средства, способы и принципы построения систем защиты информации автоматизированных систем; программно-аппаратные средства</p>	
--	--	--	---	---	--

				<p>обеспечения защиты информации в программном обеспечении автоматизированных систем; основные информационные технологии, используемые в автоматизированных системах; основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; национальные, межгосударственные и международные стандарты в области защиты информации; основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; правила оформления заявок на разработку информационных систем; основные принципы моделирования; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем; принципы формирования и реализации политики безопасности информации в автоматизированных системах; национальные, межгосударственные и международные стандарты в области защиты информации; способы реализации угроз безопасности в автоматизированных системах; последствия от нарушения свойств безопасности информации; принципы формирования и реализации политики безопасности информации в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации; программно-аппаратные средства обеспечения защиты информации автоматизированных систем; методы сбора и анализа научно-технической информации в области защиты информации; методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем; основные способы применения математических моделей при проектировании систем</p>	
--	--	--	--	--	--

			<p>защиты информации автоматизированных систем; основные меры по защите информации в автоматизированных системах; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; средства и методы хранения и передачи информации; нормативную базу, регламентирующую создание и эксплуатацию ИАС; назначение и классификацию информационных и аналитических систем, систем управления; структуру функциональной и обеспечивающих частей ИАС; методы проектирования ИАС; принципы построения защищенных телекоммуникационных систем; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; нормативные правовые акты в области защиты информации; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; критерии и показатели эффективности ИАС; методологические основы, методы и средства математического моделирования ИАС; методы теории вероятностей, теории случайных процессов и математической статистики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.</p> <p><b>Умеет на базовом уровне, с ошибками:</b></p> <p>определить суть проблемной ситуации и этапы ее разрешения с учетом вариативных контекстов; осуществлять сбор, систематизацию и критический анализ информации, необходимой для выработки стратегии действий по разрешению проблемной ситуации; проводит оценку адекватности и достоверности информации о проблемной ситуации, умеет работать с противоречивой информацией из разных источников; осуществляет поиск решений проблемной ситуации на основе действий, эксперимента и опыта; критически оценивает возможные варианты решения проблемной ситуации на основе анализа причинно-следственных связей; осуществляет и аргументирует выбор стратегии по решению проблемной ситуации, оценивает преимущества и недостатки выбранной стратегии; осуществляет разработку плана действий по решению проблемной ситуации, определяет и оценивает практические</p>	
--	--	--	---	--

				<p>последствия реализации действий по разрешению проблемной ситуации; строить и структурировать жизненный цикл проекта; применяет основные процедуры и методы управления проектами и подготовки проектных решений; планировать реализацию проекта; оценивать эффективности проектов; измерять и анализировать результаты проектной деятельности; определять роль каждого участника команды; ставить перед каждым участником команды четко сформулированную задачу с учетом его роли; выбирать методы организации работы команды с учетом специфики поставленной цели, временных и прочих ограничений; составлять планы и графики основных шагов по достижению поставленной перед командой цели и оценивать необходимые временные, информационные и другие ресурсы; поддерживать в команде атмосферу сотрудничества и достижения цели, показывая ценность вклада каждого участника; предоставлять эффективную обратную связь участникам команды по промежуточным и конечным результатам работы; выявлять конфликты, возникающие в процессе командной работы, и конструктивно управлять ими; использовать различные типы коммуникации для обеспечения эффективного взаимодействия участников команды, в том числе – виртуальной; самостоятельно находит и обрабатывает информацию, необходимую для качественного выполнения академических и профессиональных задач и достижения профессионально значимых целей, в т.ч. на иностранном языке; составляет, редактирует на государственном языке РФ и/или иностранном языке, выполняет корректный перевод с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный язык различных академических и профессиональных текстов; владеет навыками и умениями установления и развития академических и профессиональных контактов, в т.ч. в международной среде, в соответствии с целями, задачами и условиями совместной деятельности, включая обмен информацией и выработку единой стратегии взаимодействия; воспринимает и анализирует информацию на государственном языке РФ и иностранном языке в процессе академического и профессионального взаимодействия; принимает участие в академических и профессиональных дискуссиях на государственном языке РФ и/или иностранном языке, аргументированно отстаивая свои позиции и идеи; анализировать разнообразие культур в процессе межкультурного взаимодействия; учитывать разнообразие культур в процессе</p>	
--	--	--	--	--	--

			<p>межкультурного взаимодействия; строить межкультурное взаимодействие с учетом разнообразия культур; оценить возможности реализации собственных профессиональных целей и расставить приоритеты; провести анализ результатов своей социальной и профессиональной деятельности; корректировать планы личного и профессионального развития;</p> <p>осуществлять подбор сетевого оборудования для конкретных организаций и эксплуатировать сетевое оборудование; разрабатывать и реализовывать политики работы в корпоративных сетях, проектировать и эксплуатировать локальные вычислительные сети, восстанавливать их работоспособность; разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД; проводить комплексное тестирование аппаратных и программных средств; оценивать сложность алгоритмов и вычислений; разрабатывать программное обеспечение, технические средства, базы данных и компьютерные сети с учетом требований по обеспечению защиты информации; осуществлять мониторинг и оперативное устранение уязвимостей в программном и аппаратном обеспечении, выявлять уязвимости в программном и аппаратном обеспечении; оценивать сложность алгоритмов и вычислений;</p> <p>классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации; анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами; организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем;</p> <p>классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации определять класс защищенности автоматизированных систем и ее составных частей; обосновывать требования к системам защиты информации автоматизированных систем; разрабатывать технические задания на создание подсистем защиты информации автоматизированных систем и отчетные документы согласно требованиям проектной документации; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем; исследовать модели автоматизированных</p>	
--	--	--	---	--

			<p>систем и систем защиты безопасности автоматизированных систем; определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах; документировать элементы информационных систем; определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем; исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности; анализировать программные, архитектурно-технические и схмотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем; определять эффективность применения средств информатизации; разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах; определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите; разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; обосновывать требования к системам защиты информации автоматизированных систем; выявлять основные угрозы безопасности информации и определять виды потенциальных нарушителей и их потенциалы; определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе; применять действующую нормативную базу в области обеспечения защиты информации; определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем; производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе;</p>	
--	--	--	---	--

			<p>формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы; выявлять известные уязвимости информационных систем; анализировать возможные уязвимости информационных систем; формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы; выбирать сертифицированные средства защиты информации в соответствии с требуемым уровнем защищённости; систематизировать результаты проведенных исследований; производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе; извлекать необходимые знания в области защиты информации из имеющихся источников, в том числе, на иностранном языке и анализировать её; выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации; применять математические модели при проектировании систем защиты информации автоматизированных систем; выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации; разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач; проектировать и реализовывать политику безопасности вычислительных сетей; строить инфологическую модель предметной области; выбирать эффективную технологию функционирования ИАС на базе моделирования; описывать функциональную часть ИАС; производить сравнительный анализ вариантов конфигураций и состава обеспечивающей части ИАС; выбирать состав комплекса средств защиты информации в ИАС; применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в ИАС; решать задачи исследования и оценки эффективности ИАС методами моделирования; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.</p>	
--	--	--	--	--

<p>менее 50 баллов</p>	<p>«неудовлетворительно»/ «не зачтено»</p>	<p>УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10</p>	<p>УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-3.1; УК-3.2; УК-4.1; УК-4.2; УК-4.3; УК-5.1; УК-5.2; УК-6.1; УК-6.2; ПК-1.1; ПК-1.2; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-2.5; ПК-2.6; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4; ПК-3.5; ПК-3.6; ПК-4.1; ПК-4.2; ПК-4.3; ПК-4.4; ПК-4.5; ПК-4.6; ПК-4.7; ПК-5.1; ПК-5.2; ПК-5.3; ПК-5.4; ПК-5.5; ПК-5.6; ПК-6.1; ПК-6.2; ПК-6.3; ПК-6.4; ПК-7.1; ПК-7.2; ПК-7.3; ПК-7.4; ПК-7.5; ПК-7.6;</p>	<p><b>Не знает на базовом уровне:</b> методику постановки цели и определения способов ее достижения; основные методологические подходы в сфере управления проектами; методы и модели структуризации проекта; методы управления рисками проекта на всех стадиях его жизненного цикла; основные виды проектов их специфику и особенности управления ими; способы оценки проектов с учетом факторов риска и неопределенности; основные принципы управления проектами на всех стадиях жизненного цикла; основные модели командообразования и факторы, влияющие на эффективность командной работы; основные модели командообразования и факторы, влияющие на эффективность командной работы; основные современные технологии организации деятельности команд, в том числе – виртуальных; основные методы анализа взаимодействия в команде; основные современные технологии коммуникации различного типа; принципы предоставления обратной связи; методы и способы применения информационно-коммуникационных технологий для сбора, хранения, обработки, представления и передачи информации в ситуациях академического и профессионального взаимодействия; основные концепции организации межличностного взаимодействия в информационной среде; принципы анализа и учета разнообразия культур в процессе межкультурного взаимодействия; методы анализа и учета разнообразия культур в процессе межкультурного взаимодействия; нормы межкультурного взаимодействия с учетом разнообразия культур; основные принципы мотивации и стимулирования карьерного развития; способы самооценки и самоопределения; основные типы и характеристики сетевого оборудования отечественных и ведущих мировых производителей; основные методологии проектирования политик информационной безопасности вычислительных сетей; нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схмотехнические решения основных узлов и блоков электронной аппаратуры; основные информационные технологии, используемые в автоматизированных системах; современные технологии программирования, особенности защиты информации в автоматизированных системах управления</p>	<p><b>Компетенции не сформированы</b></p>
--------------------------------	--	--	--	---	---

			<p>ПК-7.7; ПК-7.8; ПК-8.1; ПК-8.2; ПК-8.3; ПК-8.4; ПК-8.5; ПК-8.6; ПК-9.1; ПК-9.2; ПК-9.3; ПК-9.4; ПК-10.1; ПК-10.2; ПК-10.3.</p>	<p>технологическими процессами; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; методы оптимизации схемотехнических решений; виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; организационные меры по защите информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах; структуру и содержание основных разделов технических заданий на создание подсистем защиты информации автоматизированных систем; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах; основные меры по защите информации в автоматизированных системах; требования нормативных документов по обеспечению защиты информации; методы построения и принципы функционирования современных автоматизированных систем; основные средства, способы и принципы построения систем защиты информации автоматизированных систем; программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем; основные информационные технологии, используемые в автоматизированных системах; основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; национальные, межгосударственные и международные стандарты в области защиты информации; основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; правила оформления заявок на разработку информационных систем; основные принципы моделирования; принципы построения и функционирования, примеры</p>	
--	--	--	---	--	--

			<p>реализаций современных локальных и глобальных компьютерных сетей и их компонентов; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем; принципы формирования и реализации политики безопасности информации в автоматизированных системах; национальные, межгосударственные и международные стандарты в области защиты информации; способы реализации угроз безопасности в автоматизированных системах; последствия от нарушения свойств безопасности информации; принципы формирования и реализации политики безопасности информации в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации; программно-аппаратные средства обеспечения защиты информации автоматизированных систем; методы сбора и анализа научно-технической информации в области защиты информации; методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем; основные способы применения математических моделей при проектировании систем защиты информации автоматизированных систем; основные меры по защите информации в автоматизированных системах; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; средства и методы хранения и передачи информации; нормативную базу, регламентирующую создание и эксплуатацию ИАС; назначение и классификацию информационных и аналитических систем, систем управления; структуру функциональной и обеспечивающих частей ИАС; методы проектирования ИАС; принципы построения защищенных телекоммуникационных систем; основные средства и способы обеспечения информационной безопасности, принципы построения</p>	
--	--	--	--	--

			<p>систем защиты информации; нормативные правовые акты в области защиты информации; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; критерии и показатели эффективности ИАС; методологические основы, методы и средства математического моделирования ИАС; методы теории вероятностей, теории случайных процессов и математической статистики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.</p> <p><b>Не умеет на базовом уровне:</b></p> <p>определить суть проблемной ситуации и этапы ее разрешения с учетом вариативных контекстов; осуществлять сбор, систематизацию и критический анализ информации, необходимой для выработки стратегии действий по разрешению проблемной ситуации; проводит оценку адекватности и достоверности информации о проблемной ситуации, умеет работать с противоречивой информацией из разных источников; осуществляет поиск решений проблемной ситуации на основе действий, эксперимента и опыта; критически оценивает возможные варианты решения проблемной ситуации на основе анализа причинно-следственных связей; осуществляет и аргументирует выбор стратегии по решению проблемной ситуации, оценивает преимущества и недостатки выбранной стратегии; осуществляет разработку плана действий по решению проблемной ситуации, определяет и оценивает практические последствия реализации действий по разрешению проблемной ситуации; строить и структурировать жизненный цикл проекта; применяет основные процедуры и методы управления проектами и подготовки проектных решений; планировать реализацию проекта; оценивать эффективности проектов; измерять и анализировать результаты проектной деятельности; определять роль каждого участника команды; ставить перед каждым участником команды четко сформулированную задачу с учетом его роли; выбирать методы организации работы команды с учетом специфики поставленной цели, временных и прочих ограничений; составлять планы и графики основных шагов по достижению поставленной перед командой цели и оценивать необходимые временные, информационные и другие ресурсы; поддерживать в команде атмосферу сотрудничества и</p>	
--	--	--	---	--

			<p>достижения цели, показывая ценность вклада каждого участника; предоставлять эффективную обратную связь участникам команды по промежуточным и конечным результатам работы; выявлять конфликты, возникающие в процессе командной работы, и конструктивно управлять ими; использовать различные типы коммуникации для обеспечения эффективного взаимодействия участников команды, в том числе – виртуальной; самостоятельно находит и обрабатывает информацию, необходимую для качественного выполнения академических и профессиональных задач и достижения профессионально значимых целей, в т.ч. на иностранном языке; составляет, редактирует на государственном языке РФ и/или иностранном языке, выполняет корректный перевод с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный язык различных академических и профессиональных текстов; владеет навыками и умениями установления и развития академических и профессиональных контактов, в т.ч. в международной среде, в соответствии с целями, задачами и условиями совместной деятельности, включая обмен информацией и выработку единой стратегии взаимодействия; воспринимает и анализирует информацию на государственном языке РФ и иностранном языке в процессе академического и профессионального взаимодействия; принимает участие в академических и профессиональных дискуссиях на государственном языке РФ и/или иностранном языке, аргументированно отстаивая свои позиции и идеи; анализировать разнообразие культур в процессе межкультурного взаимодействия; учитывать разнообразие культур в процессе межкультурного взаимодействия; строить межкультурное взаимодействие с учетом разнообразия культур; оценить возможности реализации собственных профессиональных целей и расставить приоритеты; провести анализ результатов своей социальной и профессиональной деятельности; корректировать планы личного и профессионального развития;</p> <p>осуществлять подбор сетевого оборудования для конкретных организаций и эксплуатировать сетевое оборудование; разрабатывать и реализовывать политики работы в корпоративных сетях, проектировать и эксплуатировать локальные вычислительные сети, восстанавливать их работоспособность; разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем,</p>	
--	--	--	--	--

				<p>проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД; проводить комплексное тестирование аппаратных и программных средств; оценивать сложность алгоритмов и вычислений; разрабатывать программное обеспечение, технические средства, базы данных и компьютерные сети с учетом требований по обеспечению защиты информации; осуществлять мониторинг и оперативное устранение уязвимостей в программном и аппаратном обеспечении, выявлять уязвимости в программном и аппаратном обеспечении; оценивать сложность алгоритмов и вычислений; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации; анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами; организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации определять класс защищенности автоматизированных систем и ее составных частей; обосновывать требования к системам защиты информации автоматизированных систем; разрабатывать технические задания на создание подсистем защиты информации автоматизированных систем и отчетные документы согласно требованиям проектной документации; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем; исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных систем; определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах; документировать элементы информационных систем; определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем; исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности; анализировать программные, архитектурно-технические и схемотехнические решения</p>	
--	--	--	--	--	--

			<p>компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем; определять эффективность применения средств информатизации; разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах; определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите; разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; обосновывать требования к системам защиты информации автоматизированных систем; выявлять основные угрозы безопасности информации и определять виды потенциальных нарушителей и их потенциалы; определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе; применять действующую нормативную базу в области обеспечения защиты информации; определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем; производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе; формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы; выявлять известные уязвимости информационных систем; анализировать возможные уязвимости информационных систем; формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы; выбирать сертифицированные средства защиты информации в соответствии с требуемым уровнем защищённости; систематизировать результаты проведенных исследований; производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе; извлекать необходимые знания в области защиты информации из имеющихся</p>	
--	--	--	--	--

				<p>источников, в том числе, на иностранном языке и анализировать её; выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации; применять математические модели при проектировании систем защиты информации автоматизированных систем; выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации; разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач; проектировать и реализовывать политику безопасности вычислительных сетей; строить инфологическую модель предметной области; выбирать эффективную технологию функционирования ИАС на базе моделирования; описывать функциональную часть ИАС; производить сравнительный анализ вариантов конфигураций и состава обеспечивающей части ИАС; выбирать состав комплекса средств защиты информации в ИАС; применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в ИАС; решать задачи исследования и оценки эффективности ИАС методами моделирования; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.</p>	
--	--	--	--	---	--

## **16. Особенности прохождения практики для инвалидов и лиц с ОВЗ**

Выбор мест прохождения практики для обучающихся с ограниченными возможностями здоровья осуществляется с учетом рекомендаций медико-социальной экспертизы, отраженных в индивидуальной программе реабилитации, доступности рекомендованных условий труда для данной категории обучающихся (сюда относятся профильные доступные организации, готовые принять обучающихся, кафедры Университета).

Обучающимся с ограниченными возможностями здоровья и инвалидам необходимо написать заявление с приложением документов, подтверждающих необходимость подбора места практики с учетом их индивидуальных особенностей.

Содержание индивидуального задания для практики обсуждается обучающимся совместно с руководителем практики от организации, учитывая специфику организации и возможности в предоставлении материалов по отдельным аспектам организационной работы.

Обучающиеся должны проходить практику в соответствии с планом, выполняя все задания и по возникающим вопросам обращаться к руководителю практики от кафедры, сообщая о результатах проведенной работы не реже, чем два раза в неделю, при личном посещении или по электронной почте.

**Типовые задания, необходимые для оценки знаний, умений, характеризующих этапы формирования компетенций в процессе прохождения практики.**

### **Типовые общие задания на проектно-технологическую практику**

Общее задание на проектно-технологическую практику включает в себя решение и детальный разбор практических задач по управлению информационной безопасностью СЭД, применение системного подхода к проектированию системы защиты информации. Проведение аналитических исследований основных характеристик информационной безопасности, оценка уровня зрелости процессов защиты информации СЭД. В ходе общего задания студенты должны ознакомиться с направлениями защиты информации СЭД и приобрести практический опыт внедрения предлагаемых проектных решений защиты информационного пространства СЭД.

В рамках производственной практики: проектно-технологической практики проводятся мероприятия, способствующие окончательному выбору студентами направлений диссертационных исследований. В ходе выполнения общего задания обучающемуся надлежит выбрать объект научных исследований.

Объектами научных исследований являются:

- информационное пространство субъектов экономической деятельности (СЭД);
- система защиты информации СЭД;
- обеспечение информационной безопасности СЭД;
- управление информационной безопасностью СЭД;
- аудит информационной безопасности СЭД;
- информационное противоборство СЭД;
- деловая разведка СЭД;
- конкурентная разведка СЭД.

### **Типовое индивидуальное задание**

Каждому обучающемуся необходимо в зависимости от выбранного объекта исследований, а также задания разработанного и выданного к выполнению руководителем практики выполнить индивидуальное задание, результаты которого разместить в отчете.

• В рамках проектно-технологической практики у студентов должны быть сформированы умения и навыки практической работы.

В ходе выполнения индивидуального задания обучающейся может ознакомиться со следующими вопросами, имеющими отношение непосредственно к полученному заданию:

История создания организации, ее общая характеристика, организационно-правовая форма. Учредительные документы, организационная структура. Характеристика основных структурных подразделений и их задачи. Основные экономические показатели деятельности организации. Ее производственно-хозяйственные связи, партнеры и конкуренты. Основные информационные активы, подлежащие защите. Структурирование защищаемой информации. Угрозы информационной безопасности компании. Структура политики информационной безопасности компании. Система информационной безопасности компании и т. д.

### **Примеры индивидуальных заданий**

1. Разработка проекта структуры политики информационной безопасности СЭД.
2. Знакомство с документацией по безопасности электронного документооборота компании.
3. Изучение технических особенностей и выявление уязвимостей средств обработки

- информации в конкретном подразделении компании».
4. Проведение консультационных мероприятий среди сотрудников компании по вопросам угроз социальной инженерии.
  5. Разработка проекта детализированных политик информационной безопасности (по безопасной работе в Интернет, публикация материалов в открытой печати, парольная политика и т.д.).
  6. Сбор статистических данных нарушения политики информационной безопасности компании за последние три года.

#### **Примерный перечень вопросов для защиты отчета**

1. Системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности;
2. Обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;
3. Разработка систем, комплексов, средств и технологий обеспечения информационной безопасности;
4. Разработка программ и методик, испытаний средств и систем обеспечения информационной безопасности;
5. Анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества;
6. Разработка планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей;
7. Выполнение научных исследований с применением соответствующих физических и математических методов;
8. Подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях;
9. Аудит информационной безопасности информационных систем и объектов информатизации;
10. Аттестация объектов информатизации по требованиям безопасности информации.