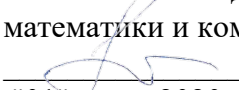


Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Романчук Иван Сергеевич
Должность: Ректор
Дата подписания: 30.03.2022 15:56:54
Уникальный программный ключ:
6319edc2b582ffdacea443f01d5779368d0957ac34f5cd074d81181530452479

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
 /М.Н. Перевалова/
"01" июня 2020 г.

УЧЕБНО-ЛАБОРАТОРНЫЙ ПРАКТИКУМ
Рабочая программа практики
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределённых компьютерных систем»
форма обучения очная

Нестерова О.А. Учебно-лабораторный практикум. Рабочая программа практики для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределённых компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа практики опубликована на сайте ТюмГУ: Учебно-лабораторный практикум [электронный ресурс] : Режим доступа: <http://www.utmn.ru/sveden/education/#>.

1. Пояснительная записка

Учебно-лабораторный практикум является первой практикой в цикле практик и направлен на ознакомление с практической работой в организации. Программа предусматривает прохождение студентом практики как в любом подразделении университета, так и в любой организации (базе практики), с которой заключен договор о прохождении студентом практики. Проводится в форме индивидуальной или групповой самостоятельной работы. Студентам предоставляется право самостоятельного выбора учреждения или организации, в которой они планируют прохождение практики

Цель: закрепление теоретических знаний и сбор материала для выполнения научно-исследовательской работы, курсовой работы, выпускной квалификационной работы.

Основными задачами практики являются:

- приобретение навыков профессиональной работы и решения практических задач в сфере информационной безопасности;
- совершенствование навыков сбора, систематизации и анализа информации, необходимой для решения практических задач в сфере информационной безопасности;
- закрепление знаний, полученных в процессе обучения, адаптация к рынку труда;
- углубленное изучение перспективных разработок на предприятии;
- участие в выполнении проектно-конструкторских и экспериментально-исследовательских работах;
- изучение структуры предприятия и действующей на нем системы управления;
- изучение информационной структуры предприятия;
- изучение информационных технологий, используемых на предприятии;
- сбор, систематизация, обобщение материала для выпускной квалифицированной работы.

Практика в полном объёме реализуется в форме практической подготовки.

1.1. Место практики в структуре образовательной программы

Данная практика входит в блок Б2.Практики, базовая часть программы и является учебной практикой.

Практика является составной частью учебного процесса и имеет целью закрепление и углубление компетенций, достигаемых студентами в процессе обучения, приобретение необходимых навыков практической работы по изучаемой специальности.

Практика проводится в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) в части государственных требований к минимуму содержания и уровню подготовки выпускников.

При прохождении практики студент должен грамотно использовать теоретический, практический материал и методы всех дисциплин разделов Учебного цикла основной образовательной программы (УЦ ООП), изученных к моменту прохождения практики. Результаты, полученные на практике, используются для выполнения курсовой (производственная практика) или выпускной квалификационной работы (преддипломная практика).

Все практики, кроме преддипломной, являются подготовительным этапом, а преддипломная практика является завершающим этапом формирования специалиста, способного самостоятельно решать конкретные задачи в деятельности коммерческих организаций.

Для практики предшествующими дисциплинами являются все дисциплины и практики учебного плана; обеспечиваемая дисциплина Курсовая работа и Научно-исследовательская работа.

1.2. Компетенции обучающегося, формируемые в результате прохождения практики

Код и наименование компетенции (из ФГОС ВО)	Код и наименование части компетенции (при наличии паспорта компетенций)	Компонент (знаниевый:функциональный)
ОК-8 : способностью к самоорганизации и самообразованию		<p><i>знать:</i></p> <ul style="list-style-type: none"> - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; <p><i>уметь:</i></p> <ul style="list-style-type: none"> - самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
ПК-1 : способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности		<p><i>Знать:</i></p> <ul style="list-style-type: none"> • об актуальных источниках информации по проектированию ТКС; • как проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов; • принципы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. <p><i>Уметь:</i></p> <ul style="list-style-type: none"> • составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; • развернуто объяснять методику проведения измерений, достоинства, недостатки, физические принципы и законы, лежащие в основе метода измерений; • осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

<p>ПК-2 : способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований</p>		<p>Знать:</p> <ul style="list-style-type: none"> • основные законы, нормативно-правовые акты, руководящие документы, регулирующие отношения в сфере информационной безопасности <p>Уметь:</p> <ul style="list-style-type: none"> • разрабатывать базовые документы, регулирующие аспекты информационной безопасности
<p>ПК-3 : способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности</p>		<p>Знать:</p> <ul style="list-style-type: none"> • суть передачи данных в сетях интернет. • основные угрозы информационной безопасности <p>Уметь:</p> <ul style="list-style-type: none"> • составлять модель угроз для информационной системы; • ориентироваться в последних отечественных и зарубежных разработках.
<p>ПК-4 : способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем</p>		<p>Знает:</p> <p>угрозы информационной безопасности информации и модели нарушителя в АС, криптографические, программно-аппаратные и технические средства и методы защиты АС,</p> <p>Умеет:</p> <p>разрабатывать и исследовать АС</p>
<p>ПК-5 : способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации</p>		<p>Знать:</p> <ul style="list-style-type: none"> - основные угрозы, способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах <p>Уметь:</p> <ul style="list-style-type: none"> - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные активы автоматизированных систем
<p>ПК-6 : способностью участвовать в разработке проектной и технической документации</p>		<p>Знает:</p> <p>модели шифрования</p> <p>методы формирования требований по защите информации,</p> <p>Умеет:</p> <p>анализировать программные и технические компоненты с целью выявления уязвимостей</p>
<p>ПК-7 : способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ</p>		<p>Знать:</p> <p>действующие нормативные и методические документы по оформлению научно-технической документации, обзоров, отчетов и публикаций</p> <p>Уметь:</p> <p>разрабатывать научно-техническую документацию, готовить научнотехнические отчеты, обзоры,</p>

		публикации по результатам выполненных работ
ПК-8 : способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы		Знает: средства обеспечения безопасности данных, основы организационного и правового обеспечения ИБ, Умеет: формировать требования разрабатывать сертификации для программного обеспечения
ПК-9 : способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы		Знать: методы и средства построения защищенных распределенных ИС Уметь: Использовать методы и средства построения защищенных распределенных ИС
ПК-10 : способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		Знает: основные принципы и подходы в области электроники и схемотехники, программировании, Умеет: проектировать структуру и архитектуру программного обеспечения, владеть навыками проектирования программного обеспечения.
ПК-11 : способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации		Знать: принципы формирования политики информационной безопасности автоматизированных систем Уметь: разрабатывать политики информационной безопасности автоматизированных систем
ПК-12 : способностью проводить инструментальный мониторинг защищенности компьютерных систем		Знать: процессы и процедуры планирования системы управления информационной безопасностью автоматизированной системы Уметь: использовать рискориентированную методологию управления информационной безопасностью автоматизированных систем
ПК-13 : способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности		Знать: основные принципы построения распределенных ИС Уметь: проектировать распределенные ИС

<p>ПК-14 : способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа</p>		<p>Знать:</p> <ul style="list-style-type: none"> • методики контрольных проверок работоспособности и эффективности применяемы технических средств защиты информации • методики контрольных проверок работоспособности и эффективности применяемы криптографических средств защиты информации • методики контрольных проверок работоспособности и эффективности применяемы программно-аппаратных средств защиты информации <p>Уметь:</p> <ul style="list-style-type: none"> • проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации
<p>ПК-15 : способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы</p>		<p>Знать:</p> <p>знать методы проведения экспериментально-исследовательских работ по сертификации средств защиты автоматизированных систем</p> <p>Уметь:</p> <ul style="list-style-type: none"> • применять методы проведения экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем
<p>ПК-16 : способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем</p>		<p>Знать:</p> <p>рабочую техническую документацию с учетом действующих нормативных и методических документов. методы и приемы подбора, изучения и обобщения научнотехнической литературы, нормативных и методических материалов по профилю своей профессиональной</p> <p>Уметь:</p> <p>Оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов осуществлять подбор, изучение и обобщение научнотехнической литературы, нормативных и методических материалов, по профилю своей профессионально й деятельности</p>
<p>ПК-17 : способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные</p>		<p>Знать:</p> <p>знать методы синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем</p> <p>Уметь:</p>

системы, системы управления базами данных, сетевое программное обеспечение		проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем
ПК-18 : способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		Знать: необходимые настройки по при работе с программно-аппаратными средствами обеспечения информационной безопасности компьютерных систем Уметь: выполнять необходимые настройки по при работе с программно-аппаратными средствами обеспечения информационной безопасности компьютерных систем
ПК-19 : способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации		Знать: процессы и процедуры совершенствования системы управления информационной безопасностью автоматизированной системы Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем
ПК-20 : способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций		Знать: методы и средства используемые при защите информации; принципы работы средств обеспечения устойчивости ИС Уметь: проектировать и реализовывать комплексную систему управления ИС
ПСК-3.1 : способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем		Знать: правила, процедуры, методы для защиты информации ограниченного доступа Уметь: Применять правила, процедуры, методы) для защиты информации ограниченного доступа
ПСК-3.2 : способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем		Знать: средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций Уметь Эффективно применять средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций

ПСК-3.3 : способностью использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности		Знать: основные методы управления защитой информации Уметь: выбирать меры и средства защиты информации для использования их с целью обеспечения требуемого уровня защищённости автоматизированной системы
ПСК-3.4 : способностью организовывать защиту информации в распределенных компьютерных системах		Знать: методы, принципы, процедуры и службы администрирования информационных систем Уметь: участвовать в администрировании подсистемы информационной безопасности
ПСК-3.5 : способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем		Знать: основные протоколы компьютерных сетей Уметь: разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных
ОПК-3 : способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации		Знать: • технологии хранения, поиска и сортировки информации; • основные принципы поисковых алгоритмов сети интернет. Уметь: • использовать информационные, компьютерные и сетевые технологии в профессиональной деятельности; • анализировать большие массивы информации и находить достоверные факты.

2. Структура и трудоемкость практики

Семестр 6. Форма проведения практики концентрированная. Способы проведения практики стационарная. Общая трудоемкость практики составляет 3 зачетных единицы, 108 академических часов, продолжительность 2 недели.

3. Содержание практики

№ п:п	Разделы (этапы) практики	Виды работы на практике, включая самостоятельную работу студентов	Трудоемкость (в часах)	Формы текущего контроля
1	Ознакомительная встреча, инструктаж по технике безопасности	Лекция по технике безопасности	3	Проверка знаний техники безопасности

2	Определение целей и задач практики	Планирование и согласование работы с руководителем	8	Индивидуальный план работы, заполнение дневника по практике
3	Сбор информации и выполнение производственных заданий	Работа над проектом или иным заданием	72	Дневник
4	Промежуточный контроль	Промежуточный отчет	9	Дневник
5	Мероприятия обработке и систематизации фактического и литературного материала	Сбор, обработка и систематизация полученных результатов	8	Дневник
6	Сдача/защита отчета по практике	Предоставление отчета и дневника руководителю практики/ доклад о задачах и результатах практики	8	Собеседование, пояснительная записка, дневник и характеристика
Итого			108	

4. Промежуточная аттестация по практике

Форма контроля - экзамен

Контроль сформированности заявленных компетенций после прохождения практики осуществляется путем проверки теоретических знаний, практических навыков и опыта с использованием промежуточной аттестации:

- прием отчета, включающий в себя пояснительную записку, дневник и характеристику;
- прием доклада о прохождении практики (обязательность устанавливается регламентом выпускающей кафедры).

5. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по итогам прохождения практики

5.1 Критерии оценивания компетенций:

Таблица 4

Карта критериев оценивания компетенций

№ п:п	Код и наименование компетенции	Компонент (знаниевый:функциональный)	Оценочные материалы	Критерии оценивания
1	ОК-8 : способностью к самоорганизации и самообразованию	<i>знать:</i> - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте

		<p>профессиональной деятельности;</p> <p><i>уметь:</i></p> <ul style="list-style-type: none"> - самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности; 		<p>ответов на теоретические вопросы, при глубине понимания и</p>
2	<p>ПК-1 : способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности</p>	<p>Знать:</p> <ul style="list-style-type: none"> • об актуальных источниках информации по проектированию ТКС; • как проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов; • принципы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. <p>Уметь:</p> <ul style="list-style-type: none"> • составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; • развернуто объяснять методику проведения измерений, достоинства, недостатки, физические принципы и законы, лежащие в основе метода измерений; • осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности. 	<p>Собеседование, доклад, отчет о практике</p>	<p>правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»</p>
3	<p>ПК-2 : способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке</p>	<p>Знать:</p> <ul style="list-style-type: none"> • основные законы, нормативно-правовые акты, руководящие документы, регулирующие отношения в сфере информационной безопасности 	<p>Собеседование, доклад, отчет о практике</p>	

	защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	Уметь: • разрабатывать базовые документы, регулирующие аспекты информационной безопасности		
4	ПК-3 : способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знать: • суть передачи данных в сетях интернет. • основные угрозы информационной безопасности Уметь: • составлять модель угроз для информационной системы; • ориентироваться в последних отечественных и зарубежных разработках.	Собеседование, доклад, отчет о практике	
5	ПК-4 : способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знает: угрозы информационной безопасности информации и модели нарушителя в АС, криптографические, программно-аппаратные и технические средства и методы защиты АС, Умеет: разрабатывать и исследовать АС	Собеседование, доклад, отчет о практике	
6	ПК-5 : способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: - основные угрозы, способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах Уметь: - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные активы автоматизированных систем	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предложенных заданий.
7	ПК-6 : способностью участвовать в разработке проектной и технической документации	Знает: модели шифрования методы формирования требований по защите информации, Умеет: анализировать программные и технические компоненты с целью выявления уязвимостей	Собеседование, доклад, отчет о практике	Шкала критериев
8	ПК-7 : способностью разрабатывать научно-техническую документацию, готовить	Знать: действующие нормативные и методические документы по оформлению научно-	Собеседование, доклад, отчет о	В

	научно-технические отчеты, обзоры, публикации по результатам выполненных работ	технической документации, обзоров, отчетов и публикаций Уметь: разрабатывать научно-техническую документацию, готовить научнотехнические отчеты, обзоры, публикации по результатам выполненных работ	практик е	применен а согласно требован иям п. 4.29 «Положе ния о текущем контроле успеваем ости и промежут очной аттестаци и обучающ ихся ФГАОУ ВО ТюмГУ»
9	ПК-8 : способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы	Знает: средства обеспечения безопасности данных, основы организационного и правового обеспечения ИБ, Умеет: формировать требования разрабатывать сертификации для программного обеспечения	Собесед ование, доклад, отчет о практик е	
10	ПК-9 : способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	Знать: методы и средства построения защищенных распределенных ИС Уметь: Использовать методы и средства построения защищенных распределенных ИС	Собесед ование, доклад, отчет о практик е	
11	ПК-10 : способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает: основные принципы и подходы в области электроники и схемотехники, программировании, Умеет: проектировать структуру и архитектуру программного обеспечения, владеть навыками проектирования программного обеспечения.	Собесед ование, доклад, отчет о практик е	
12	ПК-11 : способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	Знать: принципы формирования политики информационной безопасности автоматизированных систем Уметь: разрабатывать политики информационной безопасности автоматизированных систем	Собесед ование, доклад, отчет о практик е	Компетен ция сформиро вана при правильн ости и полноте ответов на теоретиче

13	ПК-12 : способностью проводить инструментальный мониторинг защищенности компьютерных систем	<p>Знать: процессы и процедуры планирования системы управления информационной безопасностью автоматизированной системы</p> <p>Уметь: использовать рискориентированную методологию управления информационной безопасностью автоматизированных систем</p>	Собеседование, доклад, отчет о практике	ские вопросы, при глубине понимания и правильности выполнения предложенных заданий.
14	ПК-13 : способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности	<p>Знать: основные принципы построения распределенных ИС</p> <p>Уметь: проектировать распределенные ИС</p>	Собеседование, доклад, отчет о практике	Шкала критериев в применении согласно требованиям п.
15	ПК-14 : способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	<p>Знать:</p> <ul style="list-style-type: none"> • методики контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации • методики контрольных проверок работоспособности и эффективности применяемых криптографических средств защиты информации • методики контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации <p>Уметь:</p> <ul style="list-style-type: none"> • проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации 	Собеседование, доклад, отчет о практике	4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
16	ПК-15 : способностью разрабатывать предложения по совершенствованию системы управления информационной	<p>Знать: знать методы проведения экспериментально-исследовательских работ по сертификации средств защиты автоматизированных систем</p> <p>Уметь:</p>	Собеседование, доклад, отчет о практике	

	безопасностью компьютерной системы	<ul style="list-style-type: none"> • применять методы проведения экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем 		
17	ПК-16 : способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	<p>Знать:</p> <p>рабочую техническую документацию с учетом действующих нормативных и методических документов. методы и приемы подбора, изучения и обобщения научнотехнической литературы, нормативных и методических материалов по профилю своей профессиональной</p> <p>Уметь:</p> <p>Оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов осуществлять подбор, изучение и обобщение научнотехнической литературы, нормативных и методических материалов, по профилю своей профессиональной деятельности</p>	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предложенных заданий.
18	ПК-17 : способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	<p>Знать:</p> <p>знать методы синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем</p> <p>Уметь:</p> <p>проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p>	Собеседование, доклад, отчет о практике	Шкала критериев применения согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
19	ПК-18 : способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами	<p>Знать:</p> <p>необходимые настройки по работе с программно-аппаратными средствами обеспечения информационной безопасности компьютерных систем</p> <p>Уметь:</p> <p>выполнять необходимые настройки по работе с программно-аппаратными средствами обеспечения</p>	Собеседование, доклад, отчет о практике	Шкала критериев применения согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

	данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	информационной безопасности компьютерных систем		
20	ПК-19 : способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Знать: процессы и процедуры совершенствования системы управления информационной безопасностью автоматизированной системы Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	Собеседование, доклад, отчет о практике	
21	ПК-20 : способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	Знать: методы и средства используемые при защите информации; принципы работы средств обеспечения устойчивости ИС Уметь: проектировать и реализовывать комплексную систему управления ИС	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о
22	ПСК-3.1 : способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем	Знать: правила, процедуры, методы для защиты информации ограниченного доступа Уметь: Применять правила, процедуры, методы) для защиты информации ограниченного доступа	Собеседование, доклад, отчет о практике	
23	ПСК-3.2 : способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем	Знать: средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций Уметь Эффективно применять средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их	Собеседование, доклад, отчет о практике	

		работоспособности при возникновении нештатных ситуаций		текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО «ТюмГУ»
24	ПСК-3.3 : способностью использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности	Знать: основные методы управления защитой информации Уметь: выбирать меры и средства защиты информации для использования их с целью обеспечения требуемого уровня защищённости автоматизированной системы	Собеседование, доклад, отчет о практике	
25	ПСК-3.4 : способностью организовывать защиту информации в распределенных компьютерных системах	Знать: методы, принципы, процедуры и службы администрирования информационных систем Уметь: участвовать в администрировании подсистемы информационной безопасности	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов
26	ПСК-3.5 : способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем	Знать: основные протоколы компьютерных сетей Уметь: разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных	Собеседование, доклад, отчет о практике	на теоретические вопросы, при глубине понимания и
27	ОПК-3 : способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	Знать: • технологии хранения, поиска и сортировки информации; • основные принципы поисковых алгоритмов сети интернет. Уметь: • использовать информационные, компьютерные и сетевые технологии в профессиональной деятельности; • анализировать большие массивы информации и находить достоверные факты.	Собеседование, доклад, отчет о практике	правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежу-

				очной аттестаци и обучающ ихся ФГАОУ ВО ТюмГУ»
--	--	--	--	---

5.2 Оценочные материалы для проведения промежуточной аттестации по практике

Оценка за учебную практику выставляется руководителем практики по результатам проверки представленных документов.

В соответствии с регламентом кафедры практика может завершаться итоговой конференцией, на которой обсуждаются её результаты, анализируются успехи и недочёты в профессиональной подготовке будущих специалистов.

Доклады принимаются в установленном порядке.

1. Студент в течение 5 – 10 минут отчитывается о своей работе.
2. Студент отвечает на возникшие в ходе защиты вопросы и замечания по представленным документам.
3. После сдачи отчета, проверки всех документов, представленных им к защите, принимается и объявляется решение о выставлении оценки.

В отчет по практике входят:

1. Характеристика с оценкой с места основной базы практики, с подписями научного руководителя и руководителя практики от университета, а также печатью учреждения. В характеристике должно быть зафиксировано время прохождения практики, виды выполненных студентом работ, качественная характеристика работы практиканта.
2. Индивидуальный план работы студента на практике должен отражать деятельность, которые студент осуществлял в ходе практики
3. Дневник практики, в котором студент фиксирует дату, время, виды выполняемой им деятельности.
4. Пояснительная записка отражает фактическую деятельность студентов, качество выполнения заданий, предусмотренных практикой, ее целей, задач, содержания и методов, систематичность работы в ходе практики.

5.3 Система оценивания

Отчет по практике оценивается по пятибалльной шкале РФ.

Работа считается выполненной, если вовремя представлен в соответствии с требованиями отчет о практике, включающий в себя все необходимые документы. Отчет должен раскрывать цель, задачи и этапы исследования и результат работы, соответствовать специальности и виду практики.

6. Учебно-методическое и информационное обеспечение практики

6.1. Основная литература:

1. Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие: В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Режим доступа – URL: <http://znanium.com/catalog/product/463037> (Дата обращения: 15.05.2020). - Режим доступа: по подписке.

2. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: <https://znanium.com/catalog/product/463061> (Дата обращения: 15.05.2020). - Режим доступа: по подписке.

3. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие : Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с.: 60x90 1:16. - (Высшее образование) (Переплёт 7БЦ) ISBN 978-5-369-01761-6. Режим доступа - URL: <http://znanium.com/catalog/product/957144> (Дата обращения: 15.05.2020). - Режим доступа: по подписке.

6.2. Дополнительная литература:

1. Максимов, Н.В. Компьютерные сети: учеб. пособие : Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 464 с. Режим доступа - URL: <http://znanium.com/catalog/product/792686> (15.05.2020).

2. Партыка, Т. Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - Москва : Форум: НИЦ ИНФРА-М, 2014. - 432 с.: ил.; . - (Профессиональное образование). ISBN 978-5-91134-627-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/420047> (дата обращения: 15.05.2020). – Режим доступа: по подписке.

3. Гринберг, А. С. Информационные технологии управления : учебное пособие для вузов / А. С. Гринберг, Н. Н. Горбачев, А. С. Бондаренко. — Москва : ЮНИТИ-ДАНА, 2017. — 478 с. — ISBN 5-238-00725-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/71234.html> (дата обращения: 06.04.2021). — Режим доступа: для авторизир. пользователей.

4. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: <https://doi.org/10.29039/01848-4>. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1232287> (дата обращения: 15.05.2020). – Режим доступа: по подписке.

5. Дадян, Э. Г. Методы, модели, средства хранения и обработки данных: учебник : Э.Г. Дадян, Ю.А. Зеленков. — М.: Вузовский учебник: ИНФРА-М, 2017. — 168 с.; [Электронный ресурс]. - URL: <http://znanium.com/catalog/product/543943> (15.05.2020).

6. Жуков, В. Г. Безопасность вычислительных сетей. Ч. I. Базовые протоколы стека TCP/IP [Электронный ресурс] : учеб. пособие / В. Г. Жуков. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 124 с. - Текст : электронный. - URL: <https://znanium.com/catalog/product/463062> (дата обращения: 15.05.2020). – Режим доступа: по подписке.

6.3. Интернет-ресурсы:

- вузовские электронно-библиотечные системы учебной литературы;
- база научно-технической информации ВИНТИ РАН;
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru.
- методические рекомендации по оформлению отчета по практике <https://sites.google.com/view/iprpractice>

- Трудовой кодекс Российской Федерации: по состоянию на 1 апреля 2014 г. - Москва: Проспект, 2014.-224 с. . Режим доступа - URL: http://www.consultant.ru/document/cons_doc_LAW_34683/ (15.05.2020).

7. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

- Лицензионное ПО:
- Среда для электронного обучения Microsoft Teams;
- Microsoft Office;

Студент использует то программное обеспечение, которое имеется на предприятии, на котором он проходит практику.

8. Материально-техническая база для проведения практики

Целиком и полностью определяется задачами, поставленными перед студентом-практикантом руководителями практики. К нему могут относиться: полигоны, лаборатории, специально оборудованные кабинеты, измерительные и вычислительные комплексы, транспортные средства, бытовые помещения, соответствующие действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении работ.

Для доклада требуется аудитория с проектором; ПК с установленным ПО: MS Office

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

и.о. заместителя директора Института
математики и компьютерных наук

 /М.Н. Первалова/

"01" июня 2020 г.

**ПРАКТИКА ПО ПОЛУЧЕНИЮ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И ОПЫТА
ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ**

Рабочая программа практики
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределённых компьютерных систем»
форма обучения очная

Нестерова О.А. Практика по получению профессиональных умений и опыта профессиональной деятельности. Рабочая программа практики для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределённых компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа практики опубликована на сайте ТюмГУ: Практика по получению профессиональных умений и опыта профессиональной деятельности [электронный ресурс] : Режим доступа: <http://www.utmn.ru/sveden/education/#>.

1. Пояснительная записка

Практика по получению профессиональных умений и опыта профессиональной деятельности является второй практикой в цикле практик и направлен на совершенствование практических навыков. Программа предусматривает прохождение студентом практики как в любом подразделении университета, так и в любой организации (базе практики), с которой заключен договор о прохождении студентом практики. Проводится в форме индивидуальной или групповой самостоятельной работы. Студентам предоставляется право самостоятельного выбора учреждения или организации, в которой они планируют прохождение практики.

Цель: закрепление теоретических знаний и сбор материала для выполнения научно-исследовательской работы, курсовой работы, выпускной квалификационной работы.

Основными задачами практики являются:

- приобретение навыков профессиональной работы и решения практических задач в сфере информационной безопасности;
- совершенствование навыков сбора, систематизации и анализа информации, необходимой для решения практических задач в сфере информационной безопасности;
- закрепление знаний, полученных в процессе обучения, адаптация к рынку труда;
- углубленное изучение перспективных разработок на предприятии;
- участие в выполнении проектно-конструкторских и экспериментально-исследовательских работ;
- изучение структуры предприятия и действующей на нем системы управления;
- изучение информационной структуры предприятия;
- изучение информационных технологий, используемых на предприятии;
- сбор, систематизация, обобщение материала для выпускной квалифицированной работы.

Практика в полном объеме реализуется в форме практической подготовки.

1.1. Место практики в структуре образовательной программы

Данная практика входит в блок Б2.Практики, базовая часть программы и является производственной практикой.

Практика является составной частью учебного процесса и имеет целью закрепление и углубление компетенций, достигаемых студентами в процессе обучения, приобретение необходимых навыков практической работы по изучаемой специальности.

Практика проводится в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) в части государственных требований к минимуму содержания и уровню подготовки выпускников.

При прохождении практики студент должен грамотно использовать теоретический, практический материал и методы всех дисциплин разделов Учебного цикла основной образовательной программы (УЦ ООП), изученных к моменту прохождения практики. Результаты, полученные на практике, используются для выполнения курсовой (производственная практика) или выпускной квалификационной работы (преддипломная практика).

Все практики, кроме преддипломной, являются подготовительным этапом, а преддипломная практика является завершающим этапом формирования специалиста, способного самостоятельно решать конкретные задачи в деятельности коммерческих организаций.

Для практики предшествующими дисциплинами являются все дисциплины и практики учебного плана; обеспечиваемая дисциплина – Выпускная квалификационная работа.

1.2. Компетенции обучающегося, формируемые в результате прохождения практики

Код и наименование компетенции (из ФГОС ВО)	Код и наименование части компетенции <i>(при наличии паспорта компетенций)</i>	Компонент (знаниевый:функциональный)
ОК-8 : способностью к самоорганизации и самообразованию		<p>Знать:</p> <ul style="list-style-type: none"> • содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; <p>Уметь:</p> <ul style="list-style-type: none"> • самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности; • планировать цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения.
ПК-1 : способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности		<p>Знать:</p> <ul style="list-style-type: none"> • об актуальных источниках информации по проектированию ТКС; • как проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов; • принципы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. <p>Уметь:</p> <ul style="list-style-type: none"> • составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; • развернуто объяснять методику проведения измерений, достоинства, недостатки, физические принципы и законы, лежащие в основе метода измерений;

		<ul style="list-style-type: none"> • осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.
<p>ПК-2 : способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований</p>		<p>Знать:</p> <ul style="list-style-type: none"> • основные законы, нормативно-правовые акты, руководящие документы, регулирующие отношения в сфере информационной безопасности <p>Уметь:</p> <ul style="list-style-type: none"> • разрабатывать базовые документы, регулирующие аспекты информационной безопасности
<p>ПК-3 : способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности</p>		<p>Знать:</p> <ul style="list-style-type: none"> • суть передачи данных в сетях интернет. • основные угрозы информационной безопасности <p>Уметь:</p> <ul style="list-style-type: none"> • составлять модель угроз для информационной системы; • ориентироваться в последних отечественных и зарубежных разработках.
<p>ПК-4 : способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем</p>		<p>Знает:</p> <p>угрозы информационной безопасности информации и модели нарушителя в АС, криптографические, программно-аппаратные и технические средства и методы защиты АС,</p> <p>Умеет:</p> <p>разрабатывать и исследовать АС</p>
<p>ПК-5 : способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства</p>		<p>Знать:</p> <ul style="list-style-type: none"> - основные угрозы, способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах <p>Уметь:</p> <ul style="list-style-type: none"> - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные активы автоматизированных систем

криптографической защиты информации		
ПК-6 : способностью участвовать в разработке проектной и технической документации		Знает: модели шифрования методы формирования требований по защите информации, Умеет: анализировать программные и технические компоненты с целью выявления уязвимостей
ПК-7 : способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ		Знать: действующие нормативные и методические документы по оформлению научно-технической документации, обзоров, отчетов и публикаций Уметь: разрабатывать научно-техническую документацию, готовить научнотехнические отчеты, обзоры, публикации по результатам выполненных работ
ПК-8 : способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы		Знает: средства обеспечения безопасности данных, основы организационного и правового обеспечения ИБ, Умеет: формировать требования разрабатывать сертификации для программного обеспечения
ПК-9 : способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы		Знать: методы и средства построения защищенных распределенных ИС Уметь: Использовать методы и средства построения защищенных распределенных ИС
ПК-10 : способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной		Знает: основные принципы и подходы в области электроники и схемотехники, программировании, Умеет: проектировать структуру и архитектуру программного обеспечения, владеть навыками проектирования программного обеспечения.

защиты, средства криптографической защиты информации		
ПК-11 : способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации		<p>Знать:</p> <p>принципы формирования политики информационной безопасности автоматизированных систем</p> <p>Уметь:</p> <p>разрабатывать политики информационной безопасности автоматизированных систем</p>
ПК-12 : способностью проводить инструментальный мониторинг защищенности компьютерных систем		<p>Знать:</p> <p>процессы и процедуры планирования системы управления информационной безопасностью автоматизированной системы</p> <p>Уметь:</p> <p>использовать рискориентированную методологию управления информационной безопасностью автоматизированных систем</p>
ПК-13 : способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности		<p>Знать:</p> <p>основные принципы построения распределенных ИС</p> <p>Уметь:</p> <p>проектировать распределенные ИС</p>
ПК-14 : способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа		<p>Знать:</p> <ul style="list-style-type: none"> • методики контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации • методики контрольных проверок работоспособности и эффективности применяемых криптографических средств защиты информации • методики контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации <p>Уметь:</p> <ul style="list-style-type: none"> • проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных,

		криптографических и технических средств защиты информации
ПК-15 : способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы		Знать: знать методы проведения экспериментально-исследовательских работ по сертификации средств защиты автоматизированных систем Уметь: • применять методы проведения экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем
ПК-16 : способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем		Знать: рабочую техническую документацию с учетом действующих нормативных и методических документов. методы и приемы подбора, изучения и обобщения научнотехнической литературы, нормативных и методических материалов по профилю своей профессиональной Уметь: Оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов осуществлять подбор, изучение и обобщение научнотехнической литературы, нормативных и методических материалов, по профилю своей профессиональной деятельности
ПК-17 : способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение		Знать: знать методы синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем Уметь: проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем
ПК-18 : способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения		Знать: необходимые настройки по при работе с программно-аппаратными средствами обеспечения информационной безопасности компьютерных систем

<p>информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации</p>		<p>Уметь: выполнять необходимые настройки по при работе с программно-аппаратными средствами обеспечения информационной безопасности компьютерных систем</p>
<p>ПК-19 : способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации</p>		<p>Знать: процессы и процедуры совершенствования системы управления информационной безопасностью автоматизированной системы Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем</p>
<p>ПК-20 : способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций</p>		<p>Знать: методы и средства используемые при защите информации; принципы работы средств обеспечения устойчивости ИС Уметь: проектировать и реализовывать комплексную систему управления ИС</p>
<p>ПСК-3.1 : способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем</p>		<p>Знать: правила, процедуры, методы для защиты информации ограниченного доступа Уметь: Применять правила, процедуры, методы) для защиты информации ограниченного доступа</p>
<p>ПСК-3.2 : способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности</p>		<p>Знать: средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций Уметь Эффективно применять средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций</p>

распределенных компьютерных систем		
ПСК-3.3 : способностью использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности		Знать: основные методы управления защитой информации Уметь: выбирать меры и средства защиты информации для использования их с целью обеспечения требуемого уровня защищённости автоматизированной системы
ПСК-3.4 : способностью организовывать защиту информации в распределенных компьютерных системах		Знать: методы, принципы, процедуры и службы администрирования информационных систем Уметь: участвовать в администрировании подсистемы информационной безопасности
ПСК-3.5 : способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем		Знать: основные протоколы компьютерных сетей Уметь: разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных

2. Структура и трудоемкость практики

Семестр 8. Форма проведения практики концентрированная. Способы проведения практики стационарная. Общая трудоемкость практики составляет 3 зачетных единицы, 108 академических часов, продолжительность 2 недель.

Семестр 10. Форма проведения практики концентрированная. Способы проведения практики стационарная. Общая трудоемкость практики составляет 3 зачетных единицы, 108 академических часов, продолжительность 2 недель.

Способы проведения практики:
стационарная;
выездная.

3. Содержание практики

№ п:п	Разделы (этапы) практики	Виды работы на практике, включая самостоятельную работу студентов	Трудоемкость (в часах)	Формы текущего контроля

Семестр 8				
1	Ознакомительная встреча, инструктаж по технике безопасности	Лекция по технике безопасности	3	Проверка знаний техники безопасности
2	Определение целей и задач практики	Планирование и согласование работы с руководителем	8	Индивидуальный план работы, заполнение дневника по практике
3	Сбор информации и выполнение производственных заданий	Работа над проектом или иным заданием	72	Дневник
4	Промежуточный контроль	Промежуточный отчет	9	Дневник
5	Мероприятия обработке и систематизации фактического и литературного материала	Сбор, обработка и систематизация полученных результатов	8	Дневник
6	Сдача: защита отчета по практике	Предоставление отчета и дневника руководителю практики: доклад о задачах и результатах практики	8	Собеседование, пояснительная записка, дневник и характеристика
Итого за 8 семестр			108	
Семестр 10				
1	Ознакомительная встреча, инструктаж по технике безопасности	Лекция по технике безопасности	3	Проверка знаний техники безопасности
2	Определение целей и задач практики	Планирование и согласование работы с руководителем	8	Индивидуальный план работы, заполнение дневника по практике
3	Сбор информации и выполнение производственных заданий	Работа над проектом или иным заданием	72	Дневник
4	Промежуточный контроль	Промежуточный отчет	9	Дневник
5	Мероприятия обработке и систематизации фактического и литературного материала	Сбор, обработка и систематизация полученных результатов	8	Дневник
6	Сдача: защита отчета по практике	Предоставление отчета и дневника руководителю практики: доклад	8	Собеседование, пояснительная записка,

		о задачах и результатах практики		дневник и характеристика
		Итого за 10 семестр	108	
		Итого	216	

4. Промежуточная аттестация по практике

Форма контроля - экзамен

Контроль сформированности заявленных компетенций после прохождения практики осуществляется путем проверки теоретических знаний, практических навыков и опыта с использованием промежуточной аттестации:

- прием отчета, включающий в себя пояснительную записку, дневник и характеристику;
- прием доклада о прохождении практики (обязательность устанавливается регламентом выпускающей кафедры).

5. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по итогам прохождения практики

5.1 Критерии оценивания компетенций:

Таблица 4

Карта критериев оценивания компетенций

№ п:п	Код и наименование компетенции	Компонент (знаниевый:функциональный)	Оценочные материалы	Критерии оценивания
1	ОК-8 . способностью к самоорганизации и самообразованию	<p>Знать:</p> <ul style="list-style-type: none"> • содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; <p>Уметь:</p> <ul style="list-style-type: none"> • самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности; • планировать 	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации»

		цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения.		обучающихся ФГАОУ ВО ТЮМГУ»
2	ПК-1 . способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	<p>Знать:</p> <ul style="list-style-type: none"> • об актуальных источниках информации по проектированию ТКС; • как проводить анализ информационно й безопасности объектов и систем с использованием отечественных и зарубежных стандартов; • принципы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационно й безопасности по профилю своей профессиональн ой деятельности. <p>Уметь:</p> <ul style="list-style-type: none"> • составлять 	Собеседовани е, доклад, отчет о практике	

		<p>обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;</p> <ul style="list-style-type: none"> • развернуто объяснять методику проведения измерений, достоинства, недостатки, физические принципы и законы, лежащие в основе метода измерений; • осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности. 		
3	<p>ПК-2 . способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований</p>	<p>Знать:</p> <ul style="list-style-type: none"> • основные законы, нормативно-правовые акты, руководящие документы, регулирующие отношения в сфере информационной безопасности <p>Уметь:</p> <ul style="list-style-type: none"> • разрабатывать базовые документы, регулирующие 	<p>Собеседование, доклад, отчет о практике</p>	

		аспекты информационно й безопасности		
4	ПК-3 . способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знать: <ul style="list-style-type: none"> • суть передачи данных в сетях интернет. • основные угрозы информационно й безопасности Уметь: <ul style="list-style-type: none"> • составлять модель угроз для информационно й системы; • ориентироваться в последних отечественных и зарубежных разработках. 	Собеседовани е, доклад, отчет о практике	
5	ПК-4 . способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знает: угрозы информационно й безопасности информации и модели нарушителя в АС, криптографичес кие, программно- аппаратные и технические средства и методы защиты АС, Умеет: разрабатывать и исследовать АС	Собеседовани е, доклад, отчет о практике	
6	ПК-5 . способностью участвовать в разработке и конфигурировании программно- аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства	Знать: - основные угрозы, способы реализации угроз безопасности информации и модели нарушителя в автоматизирован ных системах	Собеседовани е, доклад, отчет о практике	Компетенция сформирован а при правильности и полноте ответов на теоретически е вопросы, при глубине понимания и правильности

	криптографической защиты информации	Уметь: - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные активы автоматизированных систем		выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и
7	ПК-6 . способностью участвовать в разработке проектной и технической документации	Знает: модели шифрования методы формирования требований по защите информации, Умеет: анализировать программные и технические компоненты с целью выявления уязвимостей	Собеседование, доклад, отчет о практике	промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
8	ПК-7 . способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Знать: действующие нормативные и методические документы по оформлению научно-технической документации, обзоров, отчетов и публикаций Уметь: разрабатывать научно-техническую документацию, готовить научнотехнические отчеты, обзоры, публикации по результатам	Собеседование, доклад, отчет о практике	

		выполненных работ	
9	ПК-8 . способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы	Знает: средства обеспечения безопасности данных, основы организационного и правового обеспечения ИБ, Умеет: формировать требования разрабатывать сертификации для программного обеспечения	Собеседование, доклад, отчет о практике
10	ПК-9 . способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	Знать: методы и средства построения защищенных распределенных ИС Уметь: Использовать методы и средства построения защищенных распределенных ИС	Собеседование, доклад, отчет о практике
11	ПК-10 . способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает: основные принципы и подходы в области электроники и схемотехники, программирования, Умеет: проектировать структуру и архитектуру программного обеспечения, владеть навыками проектирования программного обеспечения.	Собеседование, доклад, отчет о практике

12	ПК-11 . способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	Знать: принципы формирования политики информационной безопасности автоматизированных систем Уметь: разрабатывать политики информационной безопасности автоматизированных систем	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
13	ПК-12 . способностью проводить инструментальный мониторинг защищенности компьютерных систем	Знать: процессы и процедуры планирования системы управления информационной безопасностью автоматизированной системы Уметь: использовать рискориентированную методологию управления информационной безопасностью автоматизированных систем	Собеседование, доклад, отчет о практике	Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
14	ПК-13 . способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности	Знать: основные принципы построения распределенных ИС Уметь: проектировать распределенные ИС	Собеседование, доклад, отчет о практике	
15	ПК-14 . способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Знать: • методики контрольных проверок работоспособности и эффективности	Собеседование, доклад, отчет о практике	

		<p>применяемы технических средств защиты информации</p> <ul style="list-style-type: none"> • методики контрольных проверок работоспособнос ти и эффективности применяемы криптографичес ких средств защиты информации • методики контрольных проверок работоспособнос ти и эффективности применяемы программно- аппаратных средств защиты информации <p>Уметь:</p> <ul style="list-style-type: none"> • проводить контрольные проверки работоспособнос ти и эффективности применяемых программно- аппаратных, криптографичес ких и технических средств защиты информации 		
16	ПК-15 . способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	<p>Знать:</p> <p>знать методы проведения эксперименталь но- исследовательск их работ по сертификации средств защиты автоматизирован ных систем</p>	Собеседовани е, доклад, отчет о практике	

		<p>Уметь:</p> <ul style="list-style-type: none"> • применять методы проведения экспериментальных работ при сертификации средств защиты автоматизированных систем 		
17	<p>ПК-16 . способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем</p>	<p>Знать: рабочую техническую документацию с учетом действующих нормативных и методических документов. методы и приемы подбора, изучения и обобщения научнотехнической литературы, нормативных и методических материалов по профилю своей профессиональной</p> <p>Уметь: Оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов осуществлять подбор, изучение и обобщение научнотехнической литературы, нормативных и методических материалов, по</p>	<p>Собеседование, доклад, отчет о практике</p>	<p>Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»</p>

		профилю своей профессиональной деятельности	
18	ПК-17 . способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	Знать: знать методы синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем Уметь: проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем	Собеседование, доклад, отчет о практике
19	ПК-18 . способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: необходимые настройки по при работе с программно-аппаратными средствами обеспечения информационной безопасности компьютерных систем Уметь: выполнять необходимые настройки по при работе с программно-аппаратными средствами обеспечения информационной безопасности компьютерных систем	Собеседование, доклад, отчет о практике
20	ПК-19 . способностью производить проверки технического состояния и профилактические осмотры	Знать: процессы и процедуры совершенствования системы	Собеседование, доклад, отчет о практике

	технических средств защиты информации	управления информационно й безопасностью автоматизирован ной системы Уметь: разрабатывать предложения по совершенствованию системы управления информационно й безопасностью автоматизирован ных систем		
21	ПК-20 . способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	Знать: методы и средства используемые при защите информации; принципы работы средств обеспечения устойчивости ИС Уметь: проектировать и реализовывать комплексную систему управления ИС	Собеседовани е, доклад, отчет о практике	Компетенция сформирован а при правильности и полноте ответов на теоретически е вопросы, при глубине понимания и правильности выполнения предложенны х заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточн ой аттестации обучающихся ФГАОУ ВО ТюмГУ»
22	ПСК-3.1 . способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем	Знать: правила, процедуры, методы для защиты информации ограниченного доступа Уметь: Применять правила, процедуры, методы) для защиты информации ограниченного доступа	Собеседовани е, доклад, отчет о практике	
23	ПСК-3.2 . способностью анализировать защиту информации в распределенных	Знать: средства защиты информационно-	Собеседовани е, доклад,	

	компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем	технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций Уметь Эффективно применять средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	отчет о практике	
24	ПСК-3.3 . способностью использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности	Знать: основные методы управления защитой информации Уметь: выбирать меры и средства защиты информации для использования их с целью обеспечения требуемого уровня защищённости автоматизированной системы	Собеседование, доклад, отчет о практике	
25	ПСК-3.4 . способностью организовывать защиту информации в распределенных компьютерных системах	Знать: методы, принципы, процедуры и службы администрирования	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретически

		информационных систем Уметь: участвовать в администрировании подсистемы информационной безопасности		е вопросы, при глубине понимания и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТЮМГУ»
26	ПСК-3.5 . способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем	Знать: основные протоколы компьютерных сетей Уметь: разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных	Собеседование, доклад, отчет о практике	

5.2 Оценочные материалы для проведения промежуточной аттестации по практике

Оценка за практику выставляется руководителем практики по результатам проверки представленных документов.

В соответствии с регламентом кафедры практика может завершаться итоговой конференцией, на которой обсуждаются её результаты, анализируются успехи и недочёты в профессиональной подготовке будущих специалистов.

Доклады принимаются в установленном порядке.

1. Студент в течение 5 – 10 минут отчитывается о своей работе.
2. Студент отвечает на возникшие в ходе защиты вопросы и замечания по представленным документам.
3. После сдачи отчета, проверки всех документов, представленных им к защите, принимается и объявляется решение о выставлении оценки.

В отчет по практике входят:

1. Характеристика с оценкой с места основной базы практики, с подписями научного руководителя и руководителя практики от университета, а также печатью учреждения. В характеристике должно быть зафиксировано время прохождения практики, виды выполненных студентом работ, качественная характеристика работы практиканта.

2. Индивидуальный план работы студента на практике должен отражать деятельность, которые студент осуществлял в ходе практики

3. Дневник практики, в котором студент фиксирует дату, время, виды выполняемой им деятельности.

4. Пояснительная записка отражает фактическую деятельность студентов, качество выполнения заданий, предусмотренных практикой, ее целей, задач, содержания и методов, систематичность работы в ходе практики.

5.3 Система оценивания

Отчет по практике оценивается по пятибалльной шкале РФ.

Работа считается выполненной, если вовремя представлен в соответствии с требованиями отчет о практике, включающий в себя все необходимые документы. Отчет должен раскрывать цель, задачи и этапы исследования и результат работы, соответствовать специальности и виду практики.

6. Учебно-методическое и информационное обеспечение практики

6.1. Основная литература:

1. Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие: В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Режим доступа – URL: <http://znanium.com/catalog/product/463037> (15.05.2020).

2. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: <https://znanium.com/catalog/product/463061> (15.05.2020).

3. Максимов, Н.В. Компьютерные сети: учеб. пособие : Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 464 с. Режим доступа - URL: <http://znanium.com/catalog/product/792686> (15.05.2020).

4. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие : Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с.: 60x90 1:16. - (Высшее образование) (Переплёт 7БЦ) ISBN 978-5-369-01761-6. Режим доступа - URL: <http://znanium.com/catalog/product/957144> (15.05.2020).

6.2. Дополнительная литература:

1. Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие: В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Режим доступа – URL: <http://znanium.com/catalog/product/463037> (Дата обращения: 15.05.2020). - Режим доступа: по подписке.

2. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: <https://znanium.com/catalog/product/463061> (Дата обращения: 15.05.2020). - Режим доступа: по подписке.

3. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие : Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с.: 60x90 1:16. - (Высшее образование) (Переплёт 7БЦ) ISBN 978-5-369-01761-6. Режим доступа - URL: <http://znanium.com/catalog/product/957144> (Дата обращения: 15.05.2020). - Режим доступа: по подписке.

6.2. Дополнительная литература:

1. Максимов, Н.В. Компьютерные сети: учеб. пособие : Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 464 с. Режим доступа - URL: <http://znanium.com/catalog/product/792686> (15.05.2020).

2. Партыка, Т. Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - Москва : Форум: НИЦ ИНФРА-М, 2014. - 432 с.: ил.; . - (Профессиональное образование). ISBN 978-5-91134-627-0. - Текст : электронный. - URL:

<https://znanium.com/catalog/product/420047> (дата обращения: 15.05.2020). – Режим доступа: по подписке.

3. Гринберг, А. С. Информационные технологии управления : учебное пособие для вузов / А. С. Гринберг, Н. Н. Горбачев, А. С. Бондаренко. — Москва : ЮНИТИ-ДАНА, 2017. — 478 с. — ISBN 5-238-00725-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/71234.html> (дата обращения: 06.04.2021). — Режим доступа: для авторизир. пользователей.

4. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: <https://doi.org/10.29039/01848-4>. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1232287> (дата обращения: 15.05.2020). – Режим доступа: по подписке.

5. Дадян, Э. Г. Методы, модели, средства хранения и обработки данных: учебник : Э.Г. Дадян, Ю.А. Зеленков. — М.: Вузовский учебник: ИНФРА-М, 2017. — 168 с.; [Электронный ресурс]. - URL: <http://znanium.com/catalog/product/543943> (15.05.2020).

6. Жуков, В. Г. Безопасность вычислительных сетей. Ч. I. Базовые протоколы стека TCP/IP [Электронный ресурс] : учеб. пособие / В. Г. Жуков. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 124 с. - Текст : электронный. - URL: <https://znanium.com/catalog/product/463062> (дата обращения: 15.05.2020). – Режим доступа: по подписке.

6.3. Интернет-ресурсы:

- вузовские электронно-библиотечные системы учебной литературы;
- база научно-технической информации ВИНТИ РАН;
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru.
- методические рекомендации по оформлению отчета по практике <https://sites.google.com/view/iprpractice>
- Трудовой кодекс Российской Федерации: по состоянию на 1 апреля 2014 г. - Москва: Проспект, 2014.-224 с. . Режим доступа - URL: http://www.consultant.ru/document/cons_doc_LAW_34683/ (15.05.2020).

7. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

- **Лицензионное ПО:**
- Среда для электронного обучения Microsoft Teams;
- Microsoft Office;

Студент использует то программное обеспечение, которое имеется на предприятии, на котором он проходит практику.

8. Материально-техническая база для проведения практики


Целиком и полностью определяется задачами, поставленными перед студентом-практикантом руководителями практики. К нему могут относиться: полигоны, лаборатории, специально оборудованные кабинеты, измерительные и вычислительные комплексы, транспортные средства, бытовые помещения, соответствующие действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении работ.

Для доклада требуется аудитория с проектором; ПК с установленным ПО: MS Office

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

и.о. заместителя директора Института
математики и компьютерных наук

 /М.Н. Перевалова/

"01" июня 2020 г.

ПРЕДДИПЛОМНАЯ ПРАКТИКА

Рабочая программа практики для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределённых компьютерных систем»
форма обучения очная

Нестерова О.А. Преддипломная практика. Рабочая программа практики для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределённых компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа практики опубликована на сайте ТюмГУ: Преддипломная практика [электронный ресурс] : Режим доступа: <http://www.utmn.ru/sveden/education/#>.

1. Пояснительная записка

Преддипломная практика является последней практикой в цикле практик и направлена на подготовку выпускной квалификационной работы. Программа предусматривает прохождение студентом практики как в любом подразделении университета, так и в любой организации (базе практики), с которой заключен договор о прохождении студентом практики. Проводится в форме индивидуальной или групповой самостоятельной работы. Студентам предоставляется право самостоятельного выбора учреждения или организации, в которой они планируют прохождение практики

Цель: закрепление теоретических знаний и сбор материала для выполнения выпускной квалификационной работы.

Основными задачами практики являются:

- приобретение навыков профессиональной работы и решения практических задач в сфере информационной безопасности;
- совершенствование навыков сбора, систематизации и анализа информации, необходимой для решения практических задач в сфере информационной безопасности;
- закрепление знаний, полученных в процессе обучения, адаптация к рынку труда;
- углубленное изучение перспективных разработок на предприятии;
- участие в выполнении проектно-конструкторских и экспериментально-исследовательских работах;
- изучение структуры предприятия и действующей на нем системы управления;
- изучение информационной структуры предприятия;
- изучение информационных технологий, используемых на предприятии;
- сбор, систематизация, обобщение материала для выпускной квалифицированной работы.

Практика в полном объеме реализуется в форме практической подготовки.

1.1. Место практики в структуре образовательной программы

Данная практика входит в блок Б2.Практики, базовая часть программы и является производственной практикой.

Практика является составной частью учебного процесса и имеет целью закрепление и углубление компетенций, достигаемых студентами в процессе обучения, приобретение необходимых навыков практической работы по изучаемой специальности.

Практика проводится в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) в части государственных требований к минимуму содержания и уровню подготовки выпускников.

При прохождении практики студент должен грамотно использовать теоретический, практический материал и методы всех дисциплин разделов Учебного цикла основной образовательной программы (УЦ ООП), изученных к моменту прохождения практики. Результаты, полученные на практике, используются для выполнения курсовой (производственная практика) или выпускной квалификационной работы (преддипломная практика).

Все практики, кроме преддипломной, являются подготовительным этапом, а преддипломная практика является завершающим этапом формирования специалиста, способного самостоятельно решать конкретные задачи в деятельности коммерческих организаций.

Для практики предшествующими дисциплинами являются все дисциплины и практики учебного плана; обеспечиваемая дисциплина – Выпускная квалификационная работа.

1.2. Компетенции обучающегося, формируемые в результате прохождения практики

Код и наименование компетенции (из ФГОС ВО)	Код и наименование части компетенции <i>(при наличии паспорта компетенций)</i>	Компонент (знаниевый:функциональный)
ОК-8 : способностью к самоорганизации и самообразованию		<p><i>знать:</i></p> <ul style="list-style-type: none"> - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; <p><i>уметь:</i></p> <ul style="list-style-type: none"> - самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
ПК-1 : способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности		<p><i>Знать:</i></p> <ul style="list-style-type: none"> • об актуальных источниках информации по проектированию ТКС; • как проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов; • принципы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. <p><i>Уметь:</i></p> <ul style="list-style-type: none"> • составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; • развернуто объяснять методику проведения измерений, достоинства, недостатки, физические принципы и законы, лежащие в основе метода измерений; • осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических

		материалов по вопросам обеспечения информационной безопасности.
ПК-2 : способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований		Знать: <ul style="list-style-type: none"> • основные законы, нормативно-правовые акты, руководящие документы, регулирующие отношения в сфере информационной безопасности Уметь: <ul style="list-style-type: none"> • разрабатывать базовые документы, регулирующие аспекты информационной безопасности
ПК-3 : способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности		Знать: <ul style="list-style-type: none"> • суть передачи данных в сетях интернет. • основные угрозы информационной безопасности Уметь: <ul style="list-style-type: none"> • составлять модель угроз для информационной системы; • ориентироваться в последних отечественных и зарубежных разработках.
ПК-4 : способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем		Знает: угрозы информационной безопасности информации и модели нарушителя в АС, криптографические, программно-аппаратные и технические средства и методы защиты АС, Умеет: разрабатывать и исследовать АС
ПК-5 : способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		Знать: - основные угрозы, способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах Уметь: - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные активы автоматизированных систем
ПК-6 : способностью участвовать в разработке		Знает: модели шифрования методы формирования требований по

<p>проектной и технической документации</p>		<p>защите информации, Умеет: анализировать программные и технические компоненты с целью выявления уязвимостей</p>
<p>ПК-7 : способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ</p>		<p>Знать: действующие нормативные и методические документы по оформлению научно-технической документации, обзоров, отчетов и публикаций Уметь: разрабатывать научно-техническую документацию, готовить научнотехнические отчеты, обзоры, публикации по результатам выполненных работ</p>
<p>ПК-8 : способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы</p>		<p>Знает: средства обеспечения безопасности данных, основы организационного и правового обеспечения ИБ, Умеет: формировать требования разрабатывать сертификации для программного обеспечения</p>
<p>ПК-9 : способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы</p>		<p>Знать: методы и средства построения защищенных распределенных ИС Уметь: Использовать методы и средства построения защищенных распределенных ИС</p>
<p>ПК-10 : способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации</p>		<p>Знает: основные принципы и подходы в области электроники и схемотехники, программировании, Умеет: проектировать структуру и архитектуру программного обеспечения, владеть навыками проектирования программного обеспечения.</p>

<p>ПК-11 : способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации</p>		<p>Знать: принципы формирования политики информационной безопасности автоматизированных систем Уметь: разрабатывать политики информационной безопасности автоматизированных систем</p>
<p>ПК-12 : способностью проводить инструментальный мониторинг защищенности компьютерных систем</p>		<p>Знать: процессы и процедуры планирования системы управления информационной безопасностью автоматизированной системы Уметь: использовать рискориентированную методологию управления информационной безопасностью автоматизированных систем</p>
<p>ПК-13 : способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности</p>		<p>Знать: основные принципы построения распределенных ИС Уметь: проектировать распределенные ИС</p>
<p>ПК-14 : способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа</p>		<p>Знать: • методики контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации • методики контрольных проверок работоспособности и эффективности применяемых криптографических средств защиты информации • методики контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации Уметь: • проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p>

<p>ПК-15 : способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы</p>		<p>Знать: знать методы проведения экспериментально-исследовательских работ по сертификации средств защиты автоматизированных систем Уметь: • применять методы проведения экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем</p>
<p>ПК-16 : способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем</p>		<p>Знать: рабочую техническую документацию с учетом действующих нормативных и методических документов. методы и приемы подбора, изучения и обобщения научнотехнической литературы, нормативных и методических материалов по профилю своей профессиональной Уметь: Оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов осуществлять подбор, изучение и обобщение научнотехнической литературы, нормативных и методических материалов, по профилю своей профессиональной деятельности</p>
<p>ПК-17 : способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение</p>		<p>Знать: знать методы синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем Уметь: проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p>
<p>ПК-18 : способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные</p>		<p>Знать: необходимые настройки по при работе с программно-аппаратными средствами обеспечения информационной безопасности компьютерных систем Уметь: выполнять необходимые настройки по при работе с программно-аппаратными</p>

<p>операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации</p>		<p>средствами обеспечения информационной безопасности компьютерных систем</p>
<p>ПК-19 : способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации</p>		<p>Знать: процессы и процедуры совершенствования системы управления информационной безопасностью автоматизированной системы Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем</p>
<p>ПК-20 : способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций</p>		<p>Знать: методы и средства используемые при защите информации; принципы работы средств обеспечения устойчивости ИС Уметь: проектировать и реализовывать комплексную систему управления ИС</p>
<p>ПСК-3.1 : способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем</p>		<p>Знать: правила, процедуры, методы для защиты информации ограниченного доступа Уметь: Применять правила, процедуры, методы) для защиты информации ограниченного доступа</p>
<p>ПСК-3.2 : способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем</p>		<p>Знать: средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций Уметь Эффективно применять средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций</p>

ПСК-3.3 : способностью использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности		Знать: основные методы управления защитой информации Уметь: выбирать меры и средства защиты информации для использования их с целью обеспечения требуемого уровня защищённости автоматизированной системы
ПСК-3.4 : способностью организовывать защиту информации в распределенных компьютерных системах		Знать: методы, принципы, процедуры и службы администрирования информационных систем Уметь: участвовать в администрировании подсистемы информационной безопасности
ПСК-3.5 : способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем		Знать: основные протоколы компьютерных сетей Уметь: разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных

2. Структура и трудоемкость практики

Семестр 11. Форма проведения практики концентрированная. Способы проведения практики стационарная. Общая трудоемкость практики составляет 21 зачетная единица, 756 академических часов, продолжительность 14 недель.

Способы проведения практики:

- стационарная;
- выездная.

3. Содержание практики

№ п:п	Разделы (этапы) практики	Виды работы на практике, включая самостоятельную работу студентов	Трудоемкость (в часах)	Формы текущего контроля
1	Ознакомительная встреча, инструктаж по технике безопасности	Лекция по технике безопасности	8	Проверка знаний техники безопасности
2	Определение целей и задач практики	Планирование и согласование	14	Индивидуальный план работы,

		работы с руководителем		заполнение дневника по практике
3	Сбор информации и выполнение производственных заданий	Работа над проектом или иным заданием	678	Дневник
4	Промежуточный контроль	Промежуточный отчет	14	Дневник
5	Мероприятия обработке и систематизации фактического и литературного материала	Сбор, обработка и систематизация полученных результатов	32	Дневник
6	Сдача/защита отчета по практике	Предоставление отчета и дневника руководителю практики/ доклад о задачах и результатах практики	10	Собеседование, пояснительная записка, дневник и характеристика
Итого			756	

4. Промежуточная аттестация по практике

Форма контроля - экзамен

Контроль сформированности заявленных компетенций после прохождения практики осуществляется путем проверки теоретических знаний, практических навыков и опыта с использованием промежуточной аттестации:

- прием отчета, включающий в себя пояснительную записку, дневник и характеристику;
- прием доклада о прохождении практики (обязательность устанавливается регламентом выпускающей кафедры).

5. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по итогам прохождения практики

5.1 Критерии оценивания компетенций:

Таблица 4

Карта критериев оценивания компетенций

№ п:п	Код и наименование компетенции	Компонент (знаниевый:функциональный)	Оценочные материалы	Критерии оценивания
1	ОК-8 : способностью к самоорганизации и самообразованию	<i>знать:</i> - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности

		<p>совершенствования профессиональной деятельности;</p> <p><i>уметь:</i></p> <ul style="list-style-type: none"> - самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности; 		<p>выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»</p>
2	<p>ПК-1 : способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности</p>	<p>Знать:</p> <ul style="list-style-type: none"> • об актуальных источниках информации по проектированию ТКС; • как проводить анализ информационно й безопасности объектов и систем с использованием отечественных и зарубежных стандартов; • принципы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационно й безопасности по профилю своей профессиональной деятельности. <p>Уметь:</p>	<p>Собеседование, доклад, отчет о практике</p>	

		<ul style="list-style-type: none"> • составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; • развернуто объяснять методику проведения измерений, достоинства, недостатки, физические принципы и законы, лежащие в основе метода измерений; • осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности. 		
3	ПК-2 : способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	<p>Знать:</p> <ul style="list-style-type: none"> • основные законы, нормативно-правовые акты, руководящие документы, регулирующие отношения в сфере информационной безопасности <p>Уметь:</p> <ul style="list-style-type: none"> • разрабатывать базовые документы, 	Собеседование, доклад, отчет о практике	

		регулирующие аспекты информационно й безопасности		
4	ПК-3 : способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знать: <ul style="list-style-type: none"> • суть передачи данных в сетях интернет. • основные угрозы информационно й безопасности Уметь: <ul style="list-style-type: none"> • составлять модель угроз для информационно й системы; • ориентироваться в последних отечественных и зарубежных разработках. 	Собеседование, доклад, отчет о практике	
5	ПК-4 : способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знает: угрозы информационно й безопасности информации и модели нарушителя в АС, криптографические, программно-аппаратные и технические средства и методы защиты АС, Умеет: разрабатывать и исследовать АС	Собеседование, доклад, отчет о практике	
6	ПК-5 : способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства	Знать: - основные угрозы, способы реализации угроз безопасности информации и модели нарушителя в автоматизирован	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и

	криптографической защиты информации	ных системах Уметь: - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные активы автоматизированных систем		правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и
7	ПК-6 : способностью участвовать в разработке проектной и технической документации	Знает: модели шифрования методы формирования требований по защите информации, Умеет: анализировать программные и технические компоненты с целью выявления уязвимостей	Собеседование, доклад, отчет о практике	промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
8	ПК-7 : способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Знать: действующие нормативные и методические документы по оформлению научно-технической документации, обзоров, отчетов и публикаций Уметь: разрабатывать научно-техническую документацию, готовить научнотехнические отчеты, обзоры, публикации по	Собеседование, доклад, отчет о практике	

		результатам выполненных работ		
9	ПК-8 : способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы	Знает: средства обеспечения безопасности данных, основы организационного и правового обеспечения ИБ, Умеет: формировать требования разрабатывать сертификации для программного обеспечения	Собеседование, доклад, отчет о практике	
10	ПК-9 : способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	Знать: методы и средства построения защищенных распределенных ИС Уметь: Использовать методы и средства построения защищенных распределенных ИС	Собеседование, доклад, отчет о практике	
11	ПК-10 : способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает: основные принципы и подходы в области электроники и схемотехники, программирования, Умеет: проектировать структуру и архитектуру программного обеспечения, владеть навыками проектирования	Собеседование, доклад, отчет о практике	

		программного обеспечения.		
12	ПК-11 : способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	Знать: принципы формирования политики информационной безопасности автоматизированных систем Уметь: разрабатывать политики информационной безопасности автоматизированных систем	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
13	ПК-12 : способностью проводить инструментальный мониторинг защищенности компьютерных систем	Знать: процессы и процедуры планирования системы управления информационной безопасностью автоматизированной системы Уметь: использовать рискориентированную методологию управления информационной безопасностью автоматизированных систем	Собеседование, доклад, отчет о практике	
14	ПК-13 : способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности	Знать: основные принципы построения распределенных ИС Уметь: проектировать распределенные ИС	Собеседование, доклад, отчет о практике	
15	ПК-14 : способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Знать: • методики контрольных проверок работоспособнос	Собеседование, доклад, отчет о практике	

		<p>ти и эффективности применяемых технических средств защиты информации</p> <ul style="list-style-type: none"> • методики контрольных проверок работоспособности и эффективности применяемых криптографических средств защиты информации • методики контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации <p>Уметь:</p> <ul style="list-style-type: none"> • проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации 		
16	ПК-15 : способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	<p>Знать:</p> <p>знать методы проведения экспериментальных исследовательских работ по сертификации средств защиты</p>	Собеседование, доклад, отчет о практике	

		<p>автоматизированных систем</p> <p>Уметь:</p> <ul style="list-style-type: none"> • применять методы проведения экспериментальных исследований при сертификации средств защиты автоматизированных систем 		
17	<p>ПК-16 : способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем</p>	<p>Знать:</p> <p>рабочую техническую документацию с учетом действующих нормативных и методических документов. методы и приемы подбора, изучения и обобщения научнотехнической литературы, нормативных и методических материалов по профилю своей профессиональной</p> <p>Уметь:</p> <p>Оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов осуществлять подбор, изучение и обобщение научнотехнической литературы, нормативных и</p>	<p>Собеседование, доклад, отчет о практике</p>	<p>Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»</p>

		методических материалов, по профилю своей профессиональной деятельности	
18	ПК-17 : способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	Знать: знать методы синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем Уметь: проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем	Собеседование, доклад, отчет о практике
19	ПК-18 : способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: необходимые настройки по при работе с программно-аппаратными средствами обеспечения информационной безопасности компьютерных систем Уметь: выполнять необходимые настройки по при работе с программно-аппаратными средствами обеспечения информационной безопасности компьютерных систем	Собеседование, доклад, отчет о практике
20	ПК-19 : способностью производить проверки технического состояния и	Знать: процессы и процедуры	Собеседование, доклад,

	профилактические осмотры технических средств защиты информации	совершенствования системы управления информационной безопасностью автоматизированной системы Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	отчет о практике	
21	ПК-20 : способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	Знать: методы и средства используемые при защите информации; принципы работы средств обеспечения устойчивости ИС Уметь: проектировать и реализовывать комплексную систему управления ИС	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
22	ПСК-3.1 : способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем	Знать: правила, процедуры, методы для защиты информации ограниченного доступа Уметь: Применять правила, процедуры, методы) для защиты информации ограниченного доступа	Собеседование, доклад, отчет о практике	согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

23	<p>ПСК-3.2 : способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем</p>	<p>Знать: средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций Уметь Эффективно применять средства защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций</p>	<p>Собеседование, доклад, отчет о практике</p>	
24	<p>ПСК-3.3 : способностью использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности</p>	<p>Знать: основные методы управления защитой информации Уметь: выбирать меры и средства защиты информации для использования их с целью обеспечения требуемого уровня защищённости автоматизированной системы</p>	<p>Собеседование, доклад, отчет о практике</p>	
25	<p>ПСК-3.4 : способностью организовывать защиту информации в распределенных компьютерных системах</p>	<p>Знать: методы, принципы, процедуры и</p>	<p>Собеседование, доклад, отчет о практике</p>	<p>Компетенция сформирована при правильности</p>

		службы администрирования информационных систем Уметь: участвовать в администрировании подсистемы информационной безопасности		и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
26	ПСК-3.5 : способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем	Знать: основные протоколы компьютерных сетей Уметь: разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных	Собеседование, доклад, отчет о практике	

5.2 Оценочные материалы для проведения промежуточной аттестации по практике

Оценка за преддипломную практику выставляется руководителем практики по результатам проверки представленных документов.

Практика завершается итоговой конференцией, на которой обсуждаются её результаты, анализируются успехи и недочёты в профессиональной подготовке будущих специалистов.

Доклады принимаются в установленном порядке.

1. Студент в течение 5 – 10 минут отчитывается о своей работе.
2. Студент отвечает на возникшие в ходе защиты вопросы и замечания по представленным документам.
3. После сдачи отчета, проверки всех документов, представленных им к защите, принимается и объявляется решение о выставлении оценки.

В отчет по практике входят:

1. Характеристика с оценкой с места основной базы практики, с подписями научного руководителя и руководителя практики от университета, а также печатью учреждения. В характеристике должно быть зафиксировано время прохождения практики, виды выполненных студентом работ, качественная характеристика работы практиканта.

2. Индивидуальный план работы студента на практике должен отражать деятельность, которые студент осуществлял в ходе практики

3. Дневник практики, в котором студент фиксирует дату, время, виды выполняемой им деятельности.

4. Пояснительная записка отражает фактическую деятельность студентов, качество выполнения заданий, предусмотренных практикой, ее целей, задач, содержания и методов, систематичность работы в ходе практики.

5.3 Система оценивания

Отчет по практике оценивается по пятибалльной шкале РФ.

Работа считается выполненной, если вовремя представлен в соответствии с требованиями отчет о практике, включающий в себя все необходимые документы. Отчет должен раскрывать цель, задачи и этапы исследования и результат работы, соответствовать специальности и виду практики.

6. Учебно-методическое и информационное обеспечение практики

6.1. Основная литература:

1. Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие: В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Режим доступа – URL: <http://znanium.com/catalog/product/463037> (Дата обращения: 15.05.2020). - Режим доступа: по подписке.

2. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: <https://znanium.com/catalog/product/463061> (Дата обращения: 15.05.2020). - Режим доступа: по подписке.

3. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие : Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с.: 60x90 1:16. - (Высшее образование) (Переплёт 7БЦ) ISBN 978-5-369-01761-6. Режим доступа - URL: <http://znanium.com/catalog/product/957144> (Дата обращения: 15.05.2020). - Режим доступа: по подписке.

6.2. Дополнительная литература:

1. Максимов, Н.В. Компьютерные сети: учеб. пособие : Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 464 с. Режим доступа - URL: <http://znanium.com/catalog/product/792686> (15.05.2020).

2. Партыка, Т. Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - Москва : Форум: НИЦ ИНФРА-М, 2014. - 432 с.: ил.; . - (Профессиональное образование). ISBN 978-5-91134-627-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/420047> (дата обращения: 15.05.2020). – Режим доступа: по подписке.

3. Гринберг, А. С. Информационные технологии управления : учебное пособие для вузов / А. С. Гринберг, Н. Н. Горбачев, А. С. Бондаренко. — Москва : ЮНИТИ-ДАНА, 2017. — 478 с. — ISBN 5-238-00725-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/71234.html> (дата обращения: 06.04.2021). — Режим доступа: для авторизир. пользователей.

4. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: <https://doi.org/10.29039/01848-4>. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1232287> (дата обращения: 15.05.2020). – Режим доступа: по подписке.

5. Дадян, Э. Г. Методы, модели, средства хранения и обработки данных: учебник : Э.Г. Дадян, Ю.А. Зеленков. — М.: Вузовский учебник: ИНФРА-М, 2017. — 168 с.; [Электронный ресурс]. - URL: <http://znanium.com/catalog/product/543943> (15.05.2020).

6. Жуков, В. Г. Безопасность вычислительных сетей. Ч. I. Базовые протоколы стека TCP/IP [Электронный ресурс] : учеб. пособие / В. Г. Жуков. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 124 с. - Текст : электронный. - URL: <https://znanium.com/catalog/product/463062> (дата обращения: 15.05.2020). – Режим доступа: по подписке.

6.3. Интернет-ресурсы:

- вузовские электронно-библиотечные системы учебной литературы;
- база научно-технической информации ВИНТИ РАН;
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru.

- методические рекомендации по оформлению отчета по практике <https://sites.google.com/view/ipractice>

- Трудовой кодекс Российской Федерации: по состоянию на 1 апреля 2014 г. - Москва: Проспект, 2014.-224 с. . Режим доступа - URL: http://www.consultant.ru/document/cons_doc_LAW_34683/ (15.05.2020).

7. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

- **Лицензионное ПО:**
- Среда для электронного обучения Microsoft Teams;
- Microsoft Office;

Студент использует то программное обеспечение, которое имеется на предприятии, на котором он проходит практику.

8. Материально-техническая база для проведения практики

Целиком и полностью определяется задачами, поставленными перед студентом-практикантом руководителями практики. К нему могут относиться: полигоны, лаборатории, специально оборудованные кабинеты, измерительные и вычислительные комплексы, транспортные средства, бытовые помещения, соответствующие действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении работ.

Для доклада требуется аудитория с проектором; ПК с установленным ПО: MS Office