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 2020г.

ПРЕДДИПЛОМНАЯ ПРАКТИКА
Рабочая программа практики
для обучающихся по направлению подготовки
10.03.01 «Информационная безопасность»
профиль «Безопасность компьютерных систем»
форма обучения очная

Нестерова О.А. Преддипломная практика. Рабочая программа практики для обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», профиль «Безопасность 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 объёме реализуется в форме практической подготовки.

1.1. Место практики в структуре образовательной программы

Данная практика входит в блок Б2.Практики, вариативная 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 выпускной квалификационной работы.

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	Компонент (знаниевый:функциональный)

	части компетенции *(при наличии паспорта компетенций)*	
ОПК-4 : способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации		Знать: • технологии хранения, поиска и сортировки информации; • основные принципы поисковых алгоритмов сети интернет. Уметь: • использовать информационные, компьютерные и сетевые технологии в профессиональной деятельности;
ПК-1 : способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации		Знать: • принципы действия, основные параметры и характеристики программных средств защиты информации; • специфику формулировки задач профессиональной деятельности в терминах дисциплины; • принципы действия, основные параметры и характеристики программных средств защиты информации. Уметь: • поддерживать работоспособность информационных систем и технологий при сервисно – эксплуатационной деятельности; • производить правильный выбор схем и параметров криптографических систем; • использовать теоретический и практический материал, необходимый для представления задачи в терминах и понятиях изучаемой дисциплины.
ПК-2 : способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы		Знать: • основные приемы решения задач обработки текстовой и числовой информации; • основные способы и принципы представления структур данных; • принципы работы базовых криптографических алгоритмов; Уметь: • выполнять основные этапы реализации программ на компьютере; • реализовывать подходы процедурного программирования, реализацию вызова процедур в языках с блочной структурой.

программирования для решения профессиональных задач		• составлять программную модель криптографической системы.
ПК-3 : способностью администрировать подсистемы информационной безопасности объекта защиты		Знать: • механизм функционирования основных подсистем администрирования объектов защиты на уровне администратора безопасности: • методы программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности. Уметь: • администрировать подсистемы информационной безопасности в телекоммуникационных сетях и системах; • администрировать современные программные средства на объектах защиты на уровне администратора безопасности.
ПК-4 : способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты		Знать: • основные стандарты, регламентирующие управление ИБ; • принципы реализации, развития и совершенствования систем обеспечения ИБ предприятия; • основные понятия информационных сетей; • сетевые операционные системы. Уметь: • разрабатывать процессы управления ИБ, учитывающие особенности функционирование предприятия и решаемых им задач, и оценивать их эффективность; • решать задачи формализации разрабатываемых процессов управления ИБ; • разрабатывать и внедрять систему управления ИБ и оценивать ее эффективность; • создавать собственные интерфейсы и иерархии наследования, автоматически форматировать (реформатировать) код; • проектировать защищенные локальные сети; • настраивать сетевые операционные системы.
ПК-5 : способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации		Знать: • об основных этапах аттестации; • основные виды и процедуры внутриорганизационного контроля; виды управленческих решений и методы их принятия; • методы установки, настройки и обслуживания технических и программно- аппаратных средств защиты информации. Уметь: • определять требования к объектам информатизации; • выявлять проблемы при анализе конкретных ситуаций, предлагать способы их решения с учетом критериев социально-экономической эффективности, оценки рисков и возможных социально-экономических последствий; • производить установку, настройку и обслуживание технических и программно-аппаратных средств защиты информации.
ПК-6 : способностью принимать участие		Знать: • основные стандарты в области инфокоммуникационных систем и технологий;

в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации		• механизмы реализации атак в компьютерных сетях; • способы организации обработки и хранения данных; • средства и методы предотвращения и обнаружения вторжений. Уметь: • применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; • проводить анализ эффективности аппаратных вычислительных средств
ПК-7 : способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений		знать: • основные стандарты, регламентирующие управление ИБ; • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; основные понятия аппаратных средств вычислительной техники; • этапы проектирования ТКС; • основные проектные решения современных сетей и систем передачи информации и средства их защиты. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • производить выбор вычислительной системы для решения поставленной задачи; • проводить технико-экономическое обоснование проектных решений; • применять процессный подход к управлению ИБ в различных сферах деятельности; • осуществлять аппаратную реализации состава системы.
ПК-8 : способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов		Знать: • основные нормативные правовые акты в области информационной безопасности и защиты информации; • способы оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; • основные принципы выполнения математического моделирования процессов и объектов электроники; • сущность информационных процессов в системах связи и управления, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятиятического моделирования процессов и объектов электроники Уметь: • использовать стандартные пакеты прикладных программ для решения практических задач; • оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов • самостоятельно разрабатывать программные продукты по

		исследованию процессов и объектов электроники; • уметь анализировать структуры и содержания информационных процессов предприятия, определять виды и формы информации, наиболее подверженной угрозам и возможные пути реализации угроз.
ПК-10 : способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности		Знать: • основные нормативно-правовые документы, связанные с обеспечением ИБ; • анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности. Уметь: • использовать нормативно-правовые документы, связанные с обеспечением ИБ на объектах защиты • проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; • пользоваться математическим аппаратом для расчета основных параметров электромагнитной совместимости с использованием стандартных пакетов прикладных программ в совокупности средств.
ПК-11 : способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов		Знать: • основные понятия, приемы экспериментальных исследований; • основные методы обработки данных экспериментальных исследований; • основные принципы построения кодов, используемых в современных телекоммуникационных системах; • технологии и нормы обеспечения информационной безопасности телекоммуникационных систем. Уметь: • применять экспериментальные методы для решения задач создания новых перспективных средств электросвязи и информатики; • применять некоторые методы математического моделирования; • проводить анализ результатов, полученных в ходе исследований; • уметь обеспечивать информационную безопасность при интеграции в государственную информационную среду.
ПК-12 : способностью принимать участие в проведении экспериментальны х исследований системы защиты информации		Знать: • типы атак, угрожающих безопасности компьютеров и содержащихся в них данных; • методы проведения анализа защищенности автоматизированных систем; • оптимальные методы взаимодействия с клиентами для обеспечения максимальной защиты систем; • отечественные и зарубежные стандарты, основные мероприятия по защите информации от утечки. Уметь: • проводить анализ защищенности автоматизиров анных систем;

		• спроектировать политику безопасности данных и компьютерного оборудования небольшой организации; • применять программные и аппаратные средства защиты, применять отечественные и зарубежные стандарты на практике.
ПК-13 : способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации		знать: • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; • основные методы обслуживания и ремонта оборудования, используемого в телекоммуникационных сетях. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • определять цели и задачи, решаемые разрабатываемым процессам управления ИБ; • применять процессный подход к управлению ИБ в различных сферах деятельности; • разрабатывать процессы управления ИБ, учитывающие особенности функционирование предприятия и решаемых им задач, и оценивать их эффективность; • решать задачи формализации разрабатываемых процессов управления ИБ; • производить техническое обслуживание базового оборудования, используемого в телекоммуникационных сетях.
ПК-14 : способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности		знать: • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; • методы инструментальной оценки уровня защищенности информационно - телекоммуникационных систем и объектов информатизации и нормы. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • определять цели и задачи, решаемые разрабатываемым процессам управления ИБ; • применять процессный подход к управлению ИБ в различных сферах деятельности; • организовывать работу малого коллектива исполнителей в профессиональной деятельности.
ПК-15 : способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с		знать: • основные стандарты, регламентирующие управление ИБ; • приложения,службы и средства синхронизации доступа; • основные принципы организации информационных систем в соответствии с требованиями по защите информации. уметь: • разрабатывать процессы управления ИБ, учитывающие особенности функционирование предприятия и решаемых им задач, и оценивать их эффективность;

нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю		• разрабатывать и внедрять систему управления ИБ и оценивать ее эффективность; • определять необходимость разработки приложения службы и использования средств синхронизации доступа.

2. Структура и трудоемкость практики

Семестр 8. Форма проведения практики концентрированная. Способы проведения практики стационарная. Общая трудоемкость практики составляет 9 зачетных единицы, 324 академических часов, продолжительность 6 недель.

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	6	Проверка знаний техники безопасности
2	Определение целей и задач практики	Планирование и согласование работы с руководителем	12	Индивидуальный план работы, заполнение дневника по практике
3	Сбор информации и выполнение производственных заданий	Работа над проектом или иным заданием	260	Дневник
4	Промежуточный контроль	Промежуточный отчет	12	Дневник
5	Мероприятия по обработке и систематизации фактического и литературного материала	Сбор, обработка и систематизация полученных результатов	26	Дневник
6	Сдача/защита отчета по практике	Предоставление отчета и дневника руководителю практики/ доклад о задачах и	8	Собеседование, пояснительная записка, дневник и

		результатах практики		характеристика
			Итого	324	

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	ОПК-4 : способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знать: • технологии хранения, поиска и сортировки информации; • основные принципы поисковых алгоритмов сети интернет. Уметь: • использовать информационные, компьютерные и сетевые технологии в профессиональной деятельности;	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предло
2	ПК-1 : способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных	Знать: • принципы действия, основные параметры и характеристики программных средств защиты информации; • специфику формулировки задач профессиональной деятельности в терминах дисциплины; • принципы действия, основные параметры и характеристики программных средств защиты информации. Уметь:	Собеседование, доклад, отчет о практике	

	(в том числе криптографических) и технических средств защиты информации	• поддерживать работоспособность информационных систем и технологий при сервисно – эксплуатационной деятельности; • производить правильный выбор схем и параметров криптографических систем; • использовать теоретический и практический материал, необходимый для представления задачи в терминах и понятиях изучаемой дисциплины.		женных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
3	ПК-2 : способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знать: • основные приемы решения задач обработки текстовой и числовой информации; • основные способы и принципы представления структур данных; • принципы работы базовых криптографических алгоритмов; Уметь: • выполнять основные этапы реализации программ на компьютере; • реализовывать подходы процедурного программирования, реализацию вызова процедур в языках с блочной структурой. • составлять программную модель криптографической системы.	Собеседование, доклад, отчет о практике	
4	ПК-3 : способностью администрировать подсистемы информационной безопасности объекта защиты	Знать: • механизм функционирования основных подсистем администрирования объектов защиты на уровне администратора безопасности: • методы программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности. Уметь: • администрировать подсистемы информационной безопасности в телекоммуникационных сетях и системах; • администрировать современные программные средства на объектах защиты на уровне администратора безопасности.	Собеседование, доклад, отчет о практике	
5	ПК-4 : способностью участвовать в работах по реализации политики информационной безопасности, применять	Знать: • основные стандарты, регламентирующие управление ИБ; • принципы реализации, развития и совершенствования систем обеспечения ИБ предприятия; • основные понятия информационных сетей; • сетевые операционные системы. Уметь: • разрабатывать процессы управления ИБ,	Собеседование, доклад, отчет о практике	

	комплексный подход к обеспечению информационной безопасности объекта защиты	учитывающие особенности функционирование предприятия и решаемых им задач, и оценивать их эффективность; • решать задачи формализации разрабатываемых процессов управления ИБ; • разрабатывать и внедрять систему управления ИБ и оценивать ее эффективность; • создавать собственные интерфейсы и иерархии наследования, автоматически форматировать (реформатировать) код; • проектировать защищенные локальные сети; • настраивать сетевые операционные системы.		
6	ПК-5 : способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Знать: • об основных этапах аттестации; • основные виды и процедуры внутриорганизационного контроля; виды управленческих решений и методы их принятия; • методы установки, настройки и обслуживания технических и программно- аппаратных средств защиты информации. Уметь: • определять требования к объектам информатизации; • выявлять проблемы при анализе конкретных ситуаций, предлагать способы их решения с учетом критериев социально-экономической эффективности, оценки рисков и возможных социально-экономических последствий; • производить установку, настройку и обслуживание технических и программно-аппаратных средств защиты информации.	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
7	ПК-6 : способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Знать: • основные стандарты в области инфокоммуникационных систем и технологий; • механизмы реализации атак в компьютерных сетях; • способы организации обработки и хранения данных; • средства и методы предотвращения и обнаружения вторжений. Уметь: • применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; • проводить анализ эффективности аппаратных вычислительных средств	Собеседование, доклад, отчет о практике	

8	ПК-7 : способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	знать: • основные стандарты, регламентирующие управление ИБ; • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; основные понятия аппаратных средств вычислительной техники; • этапы проектирования ТКС; • основные проектные решения современных сетей и систем передачи информации и средства их защиты. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • производить выбор вычислительной системы для решения поставленной задачи; • проводить технико-экономическое обоснование проектных решений; • применять процессный подход к управлению ИБ в различных сферах деятельности; • осуществлять аппаратную реализации состава системы.	Собеседование, доклад, отчет о практике	п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
9	ПК-8 : способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знать: • основные нормативные правовые акты в области информационной безопасности и защиты информации; • способы оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; • основные принципы выполнения математического моделирования процессов и объектов электроники; • сущность информационных процессов в системах связи и управления, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятиятического моделирования процессов и объектов электроники Уметь: • использовать стандартные пакеты прикладных программ для решения практических задач; • оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов • самостоятельно разрабатывать программные продукты по исследованию процессов и объектов электроники; • уметь анализировать структуры и содержания информационных процессов предприятия, определять виды и формы информации, наиболее	Собеседование, доклад, отчет о практике	

		подверженной угрозам и возможные пути реализации угроз.		
10	ПК-10 : способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знать: • основные нормативно-правовые документы, связанные с обеспечением ИБ; • анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности. Уметь: • использовать нормативно-правовые документы, связанные с обеспечением ИБ на объектах защиты • проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; • пользоваться математическим аппаратом для расчета основных параметров электромагнитной совместимости с использованием стандартных пакетов прикладных программ в совокупности средств.	Собеседование, доклад, отчет о практике	
11	ПК-11 : способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Знать: • основные понятия, приемы экспериментальных исследований; • основные методы обработки данных экспериментальных исследований; • основные принципы построения кодов, используемых в современных телекоммуникационных системах; • технологии и нормы обеспечения информационной безопасности телекоммуникационных систем. Уметь: • применять экспериментальные методы для решения задач создания новых перспективных средств электросвязи и информатики; • применять некоторые методы математического моделирования; • проводить анализ результатов, полученных в ходе исследований; • уметь обеспечивать информационную безопасность при интеграции в государственную информационную среду.	Собеседование, доклад, отчет о практике	
12	ПК-12 : способностью принимать участие в проведении экспериментальных исследований системы	Знать: • типы атак, угрожающих безопасности компьютеров и содержащихся в них данных; • методы проведения анализа защищенности автоматизированных систем; • оптимальные методы взаимодействия с клиентами для обеспечения максимальной защиты систем; • отечественные и зарубежные стандарты, основные мероприятия по защите информации от	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте

	защиты информации	утечки. Уметь: • проводить анализ защищенности автоматизированных систем; • спроектировать политику безопасности данных и компьютерного оборудования небольшой организации; • применять программные и аппаратные средства защиты, применять отечественные и зарубежные стандарты на практике.		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-13 : способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	знать: • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; • основные методы обслуживания и ремонта оборудования, используемого в телекоммуникационных сетях. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • определять цели и задачи, решаемые разрабатываемым процессам управления ИБ; • применять процессный подход к управлению ИБ в различных сферах деятельности; • разрабатывать процессы управления ИБ, учитывающие особенности функционирование предприятия и решаемых им задач, и оценивать их эффективность; • решать задачи формализации разрабатываемых процессов управления ИБ; • производить техническое обслуживание базового оборудования, используемого в телекоммуникационных сетях.	Собеседование, доклад, отчет о практике	
14	ПК-14 : способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	знать: • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; • методы инструментальной оценки уровня защищенности информационно - телекоммуникационных систем и объектов информатизации и нормы. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • определять цели и задачи, решаемые разрабатываемым процессам управления ИБ; • применять процессный подход к управлению ИБ в различных сферах деятельности; • организовывать работу малого коллектива исполнителей в профессиональной деятельности.	Собеседование, доклад, отчет о практике	

15	ПК-15 : способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	знать: • основные стандарты, регламентирующие управление ИБ; • приложения,службы и средства синхронизации доступа; • основные принципы организации информационных систем в соответствии с требованиями по защите информации. уметь: • разрабатывать процессы управления ИБ, учитывающие особенности функционирование предприятия и решаемых им задач, и оценивать их эффективность; • разрабатывать и внедрять систему управления ИБ и оценивать ее эффективность; • определять необходимость разработки приложения службы и использования средств синхронизации доступа.	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 (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.: 60х90 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. 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.

2. Гринберг, А. С. Информационные технологии управления [Электронный ресурс] : учебное пособие : А. С. Гринберг, Н. Н. Горбачев, А. С. Бондаренко. - М.: Юнити-Дана, 2012. - 479 с. - Режим доступа: http://znanium.com/catalog/product/396629 (15.05.2020).

3. 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.

4. 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).

5. 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 ВИНИТИ 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

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 2020г.

ПРОЕКТНО-ТЕХНОЛОГИЧЕСКАЯ ПРАКТИКА
Рабочая программа практики
для обучающихся по направлению подготовки
10.03.01 «Информационная безопасность»
профиль «Безопасность компьютерных систем»
форма обучения очная

Нестерова О.А. Проектно-технологическая практика. Рабочая программа практики для обучающихся по направлению подготовки 10.03.01 «Информационная безопасность» профиль «Безопасность компьютерных систем», форма обучения очная. Тюмень, 2020

Рабочая программа практики опубликована на сайте ТюмГУ: Проектно-технологическая практика [электронный ресурс] : Режим доступа: http:::www.utmn.ru:sveden:education:#.

1. Пояснительная записка

Проектно-технологическая практика является промежуточной практикой в цикле практик и направлена 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 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, вариативная 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 *(при наличии паспорта компетенций)*	Компонент (знаниевый/функциональный)
ОПК-4 : способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты		Знать: • технологии хранения, поиска и сортировки информации; • основные принципы поисковых алгоритмов сети интернет. Уметь: • использовать информационные, компьютерные и сетевые технологии в профессиональной деятельности;
ПК-3 : способностью администрировать подсистемы информационной безопасности объекта защиты		Знать: • механизм функционирования основных подсистем администрирования объектов защиты на уровне администратора безопасности: • методы программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности. Уметь: • администрировать подсистемы информационной безопасности в телекоммуникационных сетях и системах; • администрировать современные программные средства на объектах защиты на уровне администратора безопасности.
ПК-7 : способностью проводить анализ исходных данных для проектирования подсистем и средств		знать: • основные стандарты, регламентирующие управление ИБ; • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; основные понятия аппаратных средств вычислительной техники; • этапы проектирования ТКС; • основные проектные решения современных сетей и систем передачи информации и средства их защиты.

обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений		уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • производить выбор вычислительной системы для решения поставленной задачи; • проводить технико-экономическое обоснование проектных решений; • применять процессный подход к управлению ИБ в различных сферах деятельности; • осуществлять аппаратную реализации состава системы.
ПК-8 : способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов		Знать: • основные нормативные правовые акты в области информационной безопасности и защиты информации; • способы оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; • основные принципы выполнения математического моделирования процессов и объектов электроники; • сущность информационных процессов в системах связи и управления, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятиятического моделирования процессов и объектов электроники Уметь: • использовать стандартные пакеты прикладных программ для решения практических задач; • оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов • самостоятельно разрабатывать программные продукты по исследованию процессов и объектов электроники; • уметь анализировать структуры и содержания информационных процессов предприятия, определять виды и формы информации, наиболее подверженной угрозам и возможные пути реализации угроз.
ПК-13 : способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности,		знать: • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; • основные методы обслуживания и ремонта оборудования, используемого в телекоммуникационных сетях. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • определять цели и задачи, решаемые разрабатываемым процессам управления ИБ;

управлять процессом их реализации		• применять процессный подход к управлению ИБ в различных сферах деятельности; • разрабатывать процессы управления ИБ, учитывающие особенности функционирование предприятия и решаемых им задач, и оценивать их эффективность; • решать задачи формализации разрабатываемых процессов управления ИБ; • производить техническое обслуживание базового оборудования, используемого в телекоммуникационных сетях.

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.

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	ОПК-4 : Выполняется получение данных. Подождите несколько секунд, а затем еще раз попробуйте вырезать или скопировать.	Знать: • технологии хранения, поиска и сортировки информации; • основные принципы поисковых алгоритмов сети интернет. Уметь: • использовать информационные, компьютерные и сетевые технологии в профессиональной деятельности;	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
2	ПК-3 : способностью администрировать подсистемы информационной безопасности объекта защиты	Знать: • механизм функционирования основных подсистем администрирования объектов защиты на уровне администратора безопасности: • методы программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности. Уметь: • администрировать подсистемы информационной безопасности в телекоммуникационных сетях и системах; • администрировать современные программные средства на объектах защиты на уровне администратора безопасности.	Собеседование, доклад, отчет о практике	
3	ПК-7 : способностью проводить анализ	знать: • основные стандарты, регламентирующие управление ИБ; • принципы разработки процессов	Собеседование, доклад,	

	исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; основные понятия аппаратных средств вычислительной техники; • этапы проектирования ТКС; • основные проектные решения современных сетей и систем передачи информации и средства их защиты. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • производить выбор вычислительной системы для решения поставленной задачи; • проводить технико-экономическое обоснование проектных решений; • применять процессный подход к управлению ИБ в различных сферах деятельности; • осуществлять аппаратную реализации состава системы.	отчет о практике	требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
4	ПК-8 : способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знать: • основные нормативные правовые акты в области информационной безопасности и защиты информации; • способы оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; • основные принципы выполнения математического моделирования процессов и объектов электроники; • сущность информационных процессов в системах связи и управления, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятиятического моделирования процессов и объектов электроники Уметь: • использовать стандартные пакеты прикладных программ для решения практических задач; • оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов • самостоятельно разрабатывать программные продукты по исследованию процессов и объектов электроники; • уметь анализировать структуры и	Собеседование, доклад, отчет о практике	

		содержания информационных процессов предприятия, определять виды и формы информации, наиболее подверженной угрозам и возможные пути реализации угроз.		
5	ПК-13 : способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	знать: • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; • основные методы обслуживания и ремонта оборудования, используемого в телекоммуникационных сетях. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • определять цели и задачи, решаемые разрабатываемым процессам управления ИБ; • применять процессный подход к управлению ИБ в различных сферах деятельности; • разрабатывать процессы управления ИБ, учитывающие особенности функционирование предприятия и решаемых им задач, и оценивать их эффективность; • решать задачи формализации разрабатываемых процессов управления ИБ; • производить техническое обслуживание базового оборудования, используемого в телекоммуникационных сетях.	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. 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 [Электронный ресурс] : учебное пособие : А. С. Гринберг, Н. Н. Горбачев, А. С. Бондаренко. - М.: Юнити-Дана, 2012. - 479 с. - Режим доступа: http://znanium.com/catalog/product/396629 (15.05.2020).

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 ВИНИТИ 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

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 2020г.

ПРАКТИКА ПО ПОЛУЧЕНИЮ ПЕРВИЧНЫХ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И НАВЫКОВ

Рабочая программа практики
для обучающихся по направлению подготовки
10.03.01 «Информационная безопасность»
профиль «Безопасность компьютерных систем»
форма обучения очная

Нестерова О.А. Практика по получению первичных профессиональных умений и навыков. Рабочая программа практики для обучающихся по направлению подготовки 10.03.01 «Информационная безопасность» профиль «Безопасность компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа практики опубликована на сайте ТюмГУ: Практика по получению первичных профессиональных умений и навыков [электронный ресурс] : Режим доступа: http:::www.utmn.ru:sveden:education:#.

1. Пояснительная записка

Практика по получению первичных профессиональных умений и навыков является первой практикой в цикле практик и направлена 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 Блок Б2.Практики, вариативная 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, НИР, Выпускная квалификационная 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)
ОПК-4 : способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации		Знать: • технологии хранения, поиска и сортировки информации; • основные принципы поисковых алгоритмов сети интернет. Уметь: • использовать информационные, компьютерные и сетевые технологии в профессиональной деятельности;
ПК-7 : способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений		знать: • основные стандарты, регламентирующие управление ИБ; • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; основные понятия аппаратных средств вычислительной техники; • этапы проектирования ТКС; • основные проектные решения современных сетей и систем передачи информации и средства их защиты. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • производить выбор вычислительной системы для решения поставленной задачи; • проводить технико-экономическое обоснование проектных решений; • применять процессный подход к управлению ИБ в различных сферах деятельности; • осуществлять аппаратную реализации состава системы.
ПК-8 : способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов		Знать: • основные нормативные правовые акты в области информационной безопасности и защиты информации; • способы оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; • основные принципы выполнения математического моделирования процессов и объектов электроники; • сущность информационных процессов в системах связи

		и управления, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятиятического моделирования процессов и объектов электроники Уметь: • использовать стандартные пакеты прикладных программ для решения практических задач; • оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов • самостоятельно разрабатывать программные продукты по исследованию процессов и объектов электроники; • уметь анализировать структуры и содержания информационных процессов предприятия, определять виды и формы информации, наиболее подверженной угрозам и возможные пути реализации угроз.
ПК-9 : способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности		Знать: • 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. Уметь: • 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-13 : способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации		знать: • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; • основные методы обслуживания и ремонта оборудования, используемого в телекоммуникационных сетях. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • определять цели и задачи, решаемые разрабатываемым процессам управления ИБ;

		• применять процессный подход к управлению ИБ в различных сферах деятельности; • разрабатывать процессы управления ИБ, учитывающие особенности функционирование предприятия и решаемых им задач, и оценивать их эффективность; • решать задачи формализации разрабатываемых процессов управления ИБ; • производить техническое обслуживание базового оборудования, используемого в телекоммуникационных сетях.

2. Структура и трудоемкость практики

Семестр 5. Форма проведения практики рассредоточенная. Способы проведения практики стационарная. Общая трудоемкость практики составляет 6 зачетных единиц, 216 академических часов, продолжительность 4 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	4	Проверка знаний техники безопасности
2	Определение целей и задач практики	Планирование и согласование работы с руководителем	10	Индивидуальный план работы, заполнение дневника по практике
3	Сбор информации и выполнение производственных заданий	Работа над проектом или иным заданием	172	Дневник
4	Промежуточный контроль	Промежуточный отчет	10	Дневник
5	Мероприятия обработке и систематизации фактического и литературного материала	Сбор, обработка и систематизация полученных результатов	12	Дневник
6	Сдача/защита отчета по практике	Предоставление отчета и дневника руководителю практики/ lоклад о задачах и результатах практики	8	Собеседование, пояснительная записка, дневник и характеристика
		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	ОПК-4 / способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знать: • технологии хранения, поиска и сортировки информации; • основные принципы поисковых алгоритмов сети интернет. Уметь: • использовать информационные, компьютерные и сетевые технологии в профессиональной деятельности;	Собеседование, доклад, отчет о практике	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания и правильности выполнения предложенных заданий. Шкала критерие в примене на согласно требован
2	ПК-7 / способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономическог	знать: • основные стандарты, регламентирующие управление ИБ; • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; основные понятия аппаратных средств вычислительной техники; • этапы проектирования ТКС; • основные проектные решения современных сетей и систем передачи информации и средства их защиты. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований	Собеседование, доклад, отчет о практике	

	о обоснования соответствующих проектных решений	к разрабатываемым процессами управления ИБ; • производить выбор вычислительной системы для решения поставленной задачи; • проводить технико-экономическое обоснование проектных решений; • применять процессный подход к управлению ИБ в различных сферах деятельности; • осуществлять аппаратную реализации состава системы.		иям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
3	ПК-8 / способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знать: • основные нормативные правовые акты в области информационной безопасности и защиты информации; • способы оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; • основные принципы выполнения математического моделирования процессов и объектов электроники; • сущность информационных процессов в системах связи и управления, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятиятического моделирования процессов и объектов электроники Уметь: • использовать стандартные пакеты прикладных программ для решения практических задач; • оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов • самостоятельно разрабатывать программные продукты по исследованию процессов и объектов электроники; • уметь анализировать структуры и содержания информационных процессов предприятия, определять виды и формы информации, наиболее подверженной угрозам и возможные пути реализации угроз.	Собеседование, доклад, отчет о практике	
4	ПК-9 / способностью осуществлять подбор, изучение и обобщение научно-технической литературы,	Знать: • 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,	Собеседование, доклад, отчет о практике	

	нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. Уметь: • 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.		
5	ПК-13 / способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	знать: • принципы разработки процессов управления ИБ; • подходы к интеграции системы управления ИБ в общую систему управления предприятием; • основные методы обслуживания и ремонта оборудования, используемого в телекоммуникационных сетях. уметь: • анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ; • определять цели и задачи, решаемые разрабатываемым процессам управления ИБ; • применять процессный подход к управлению ИБ в различных сферах деятельности; • разрабатывать процессы управления ИБ, учитывающие особенности функционирование предприятия и решаемых им задач, и оценивать их эффективность; • решать задачи формализации разрабатываемых процессов управления ИБ; • производить техническое обслуживание базового оборудования, используемого в телекоммуникационных сетях.	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. 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 [Электронный ресурс] : учебное пособие : А. С. Гринберг, Н. Н. Горбачев, А. С. Бондаренко. - М.: Юнити-Дана, 2012. - 479 с. - Режим доступа: http://znanium.com/catalog/product/396629 (15.05.2020).

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 ВИНИТИ 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