МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ

С.П. Вакуленко

«30» сентября 2019 г.

Кафедра: «Вычислительные системы, сети и информационная безопасность»

Авторы: Желенков Борис Владимирович, кандидат технических наук, доцент

ПРОГРАММА ПРАКТИКИ

Преддипломная практика

Направление подготовки:	10.03.01 Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	Очная
Год начала обучения:	2017

Одобрено на заседании Учебно-методической комиссии	Одобрено на заседании кафедры
Протокол № 2 «30» сентября 2019 г. Председатель учебно-методической комиссии _____ Н.А. Клычева	Протокол № 2/а «27» сентября 2019 г. Заведующий кафедрой _____ Б.В. Желенков

Москва 2019

1. Цели практики

Преддипломная практика предшествуют написанию бакалаврской выпускной квалификационной работы (ВКР) и имеет своей целью сбор и изучение материалов по теме работы, закрепление теоретических знаний, полученных за время обучения, получение практического опыта и навыков самостоятельной работы в процессе работы с актуальной научной проблемой или решении реальной инженерной задачи.

2. Задачи практики

Основными задачами преддипломной практики являются:
изучение:
- проектно-технологическую документацию, патентные и литературные источники в целях их использования при выполнении выпускной квалификационной работы;
- назначение, состав, принцип функционирования или организации проектируемого объекта (аппаратуры или программы);
- отечественные и зарубежные аналоги проектируемого объекта;
выполнение:
- сравнительный анализ возможных вариантов реализации научно-технической информации по теме исследования;
- технико-экономическое обоснование выполняемой разработки;
- реализацию некоторых из возможных путей решения поставленной в техническом задании задачи;
- анализ мероприятий по безопасности жизнедеятельности, обеспечению экологической чистоты, защите интеллектуальной собственности;
- разработку технического задания на дипломный проект по установленной стандартом форме.

Преддипломная практика формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности):
Эксплуатационная:
- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;
Проектно-технологическая:
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;

- проведение предварительного технико-экономического обоснования проектных расчетов
Экспериментально-исследовательская деятельность:
- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств
Организационно-управленческая деятельность:
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.

3. Место практики в структуре ОП ВО

Преддипломная практика (Б2.П.3) относится к вариативной части модуля Б2.
Для прохождения преддипломной практики не необходимы знания, умения и навыки, формируемые предшествующими дисциплинами за весь срок обучения согласно рабочему учебному плану подготовки бакалавров направления 10.03.01 Информационная безопасность по профилю "Безопасность компьютерных систем" (смотреть рабочие программы соответствующих дисциплин).

4. Тип практики, формы и способы ее проведения

Тип практики – Преддипломная практика.
Форма проведения практики – непрерывная.
Способ проведения – на кафедре или на предприятии (выездная либо стационарная).

Прохождение практики возможно с применением электронного обучения и дистанционных образовательных технологий.

Прохождение практики возможно, как в профильной организации, так и в Университете, или его структурных подразделениях.

5. Организация и руководство практикой

Преддипломная практика для студентов, обучающихся по направлению подготовки 10.03.01 Информационная безопасность по профилю "Безопасность компьютерных систем", проводится в соответствии с учебным планом в 4ом семестре.
Продолжительность практики – 6 недель. Трудоемкость - 3 зачетных единицы, 108 академических часов.

Преддипломная практика проводится в:
- ГВЦ ОАО «РЖД»;
- ИВЦ дорог;
- ОАО «НИИАС»;
- специальных конструкторских бюро;
- научноисследовательских институтах;
- вычислительных центрах различных государственных и коммерческих предприятий, банков;
- лабораториях кафедры;
- местах работы дипломника, техническая база которых и тематика работ отвечают требованиям, предъявляемым кафедрой к темам и содержанию ВКР.
Организация и учебно-методическое руководство преддипломной практикой студентов осуществляются кафедрой "Вычислительные системы и сети".
Во время преддипломной практики студент, помимо изучения производства, проводит по указанию руководителя предварительный анализ темы проекта, сбор материала к проекту, экспериментальные исследования и
т. д.
В конце преддипломной практики студент должен получить окончательно сформулированную тему ВКР.
Итоги преддипломной практики бакалавры должны представлять в виде отчетов, оформленных в соответствии со стандартными требованиями и заполненных бланков задания на ВКР.
Для руководства преддипломной практикой и последующим написанием ВКР каждому студенту на предприятии назначается руководитель проекта из числа специалистов, работающих с данной тематикой или начальников отделов. Если такого специалиста на предприятии нет, то руководителем назначается один из преподавателей кафедры.
Руководитель дипломного проектирования согласовывает с кафедрой тему проекта, выдает студенту задание на проектирование и следит за соответствием всех частей проекта требованиям настоящих методических указаний.
Кроме этого, назначается консультант от кафедры из числа преподавателей кафедры.
Обязанности руководителя практики:
1. оказание помощи студентам в их адаптации в организации;
2. обеспечение прохождения инструктажа по технике безопасности;
3. обеспечение студентов рабочими местами;
4. выбор и уточнение темы ВКР;

5. согласование темы ВКР с кафедрой при взаимодействии с консультантом от кафедры
6. совместное составление со студентом календарного рабочего плана прохождения практики, регулярный контроль за его соблюдением и качеством выполнения студентом заданий практики, согласование плана с консультантом;
7. проведение запланированных консультаций по программе практики;
8. предоставление студентам необходимой технической документации, инструкций, программных и аппаратных средств;
9. помощь в подборе необходимой литературы.
10. контроль за соблюдением студентами-практикантами трудовой дисциплины.

Обязанности консультанта от кафедры:
1. согласование с руководителем и студентом программы и календарного плана практики ;
2. рекомендация литературы, нормативно-законодательных актов и методических пособий, с которыми студент должен ознакомиться и воспользоваться для конкретизации действий в процессе прохождения практики;
3. оперативное консультирование студента в период прохождения практики;
4. взаимодействие с руководителем при выборе и формулировании темы ВКР;
5. контроль за выполнением студентом программы практики;
6. подготовка письменного отзыва об отчете студентов по практике;
7. участие в работе комиссии по приему отчетов по практике;
8. контроль за соблюдением требований кафедры к содержанию и оформлению отчета по практике и ВКР.

По окончании практики руководитель от организации проверяет отчет и дает оценку его содержания и качества практической работы студента.

Прохождение практики возможно, как в профильной организации, так и в Университете, или его структурных подразделениях.

В случае применения электронного обучения и дистанционных образовательных технологий при прохождении практики, руководители практики, как со стороны Университета, так и со стороны профильной организации, обеспечивают представление полного пакета справочных, методических и иных материалов, а также дистанционное консультирование обучающихся.

6. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения ОП

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
1	ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том	Знать и понимать: понятия информационной безопасности, составные элементы подсистем и их характеристики, правила эксплуатации используемых подсистем информационной безопасности, методы и средства конфигурирования и контроля

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	числе криптографических) и технических средств защиты информации	работоспособности средств безопасности, предоставляемых аппаратно-программными комплексами. Уметь: контролировать работу подсистем и изменять конфигурационные параметры при необходимости, применять методы и средства контроля работоспособности средств безопасности, предоставляемых аппаратно-программными комплексами, находить наиболее уязвимые места в системе, оценивать возможные вредоносные действия и решать задачи по минимизации вредоносных воздействий. Владеть: навыками по настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации, прогнозирования поведения подсистемы информационной безопасности объекта при изменении внешних воздействий; навыками эксплуатации подсистем управления информационной безопасностью предприятия построенных с использованием современного оборудования.
2	ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знать и понимать: стандарты по ИБ, порядок и стадии проведения аудита ИБ. Уметь: определять цели проведения аудита, моделировать угрозы, применять инструментальные необходимые средства, оформлять документацию по этапам аудита ИБ. Владеть: навыками проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
3	ПК-11 способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Знать и понимать: методики проведения экспериментов и способы оценки погрешности и достоверности полученных результатов. Уметь: выбирать необходимую методику проведения экспериментов и способ оценки погрешности и достоверности полученных результатов Владеть: навыками проведения экспериментов по заданной методике, обработки, оценки погрешности и достоверности их результатов.
4	ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Знать и понимать: методы и средства контроля работоспособности средств безопасности, предоставляемых сетевыми устройствами. Уметь: решать задачи по конфигурированию сетевого оборудования при его установке в существующую

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
		систему защиты информации; выбирать необходимые средства для проведения экспериментальных исследований системы защиты информации. Владеть: навыками использования средств, предоставляемых сетевым оборудованием и специализированными сетевыми протоколами, навыками по моделированию угроз и оценке обоснования проектных решений по обеспечению информационной безопасности; сборки и настройки полигонов для проведения экспериментальных исследований системы защиты информации.
5	ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Знать и понимать: современные комплексы мер по обеспечению информационной безопасности. Уметь: организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности. Владеть: навыками участия в формировании, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации
6	ПК-14 способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Знать и понимать: организационно-правовые методы по обеспечению информационной безопасности. Уметь: организовывать работу малого коллектива исполнителей для поддержки выполнения комплекса мер по обеспечению информационной безопасности Владеть: навыками организации работы малого коллектива исполнителей по обеспечению информационной безопасности.
7	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 и понимать: методы защиты информации, и нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Уметь: выбирать методы защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Владеть: основными методами получения обработки и хранения информации, основными приемами

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
		обнаружения и предотвращения угроз информационной безопасности; основными приемами эксплуатации вычислительных систем; навыками организации процесса 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.
8	ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знать и понимать: современные программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения задач ИБ. Уметь: выбирать необходимые программные средства системного, прикладного и специального назначения для решения задач ИБ. Владеть: навыками применения программных средств системного, прикладного и специального назначения, инструментальных средств, языки и системы программирования для решения задач ИБ.
9	ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Знать и понимать: современные средства администрирования подсистем информационной безопасности объекта защиты. Уметь: выбирать необходимые средства администрирования подсистем информационной безопасности объекта защиты. Владеть: выбирать необходимые средства администрирования подсистем информационной безопасности объекта защиты.
10	ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Знать и понимать: современные принципы разработки ИБ, процессов управления ИБ и направления их развития, основные стандарты по управлению ИБ, принципы построения СУИБ, способы формирования единой СУИБ предприятия. Уметь: анализировать текущее состояние ИБ на предприятии, определять цели и задачи, решаемые создаваемыми процессами управления ИБ; применять процессный подход к управлению к обеспечению информационной безопасности объекта защиты; разрабатывать и внедрять процессы управления ИБ с проведением оценки их эффективности. Владеть: навыками управления информационной безопасностью объектов, терминологией и методами построения СУИБ; навыками анализа информационных ресурсов, подлежащих защите и угроз ИБ и уязвимостей; навыками построения СУИБ.

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
11	ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Знать и понимать: необходимые требования к безопасности информации на объекте информатизации. Уметь: организовывать и сопровождать процесс аттестации объекта информатизации по требованиям безопасности информации Владеть: навыками в организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации и интерпретировать полученные в процессе проведения аудита результаты
12	ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Знать и понимать: эксплуатационные параметры и технические характеристики аппаратных и технических средств защиты информации. Уметь: проверять работоспособность элементов системы защиты с помощью необходимых технических средств Владеть: навыками интерпретировать полученные результаты для получения оценки эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.
13	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 и понимать: методы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, классификацию угроз и средства защиты, предоставляемые сетевым оборудованием. Уметь: выбирать необходимые средства защиты для обеспечения необходимого уровня информационной безопасности с выполнением технико-экономического обоснования Владеть: навыками анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; проведения технико-экономического обоснования проектных решений для обеспечения необходимого уровня информационной безопасности.
14	ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знать и понимать: стандарты и нормативные документы для оформления рабочей технической документации Уметь: определять стандарты, действующие нормативные и методические документы и для оформления рабочей технической документации Владеть: навыками оформления рабочей технической документации с учетом действующих нормативных и

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
		методических документов .
15	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 и понимать: основные принципы формального представления информации, понятия информационной безопасности, составные элементы подсистем и их характеристики. Уметь: искать и анализировать информацию, четко ставить цель и последовательно добиваться ее осуществления, определять уязвимости объектов защиты; осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов Владеть: навыками поиска и анализа информации, определения взаимосвязи явлений и объектов; навыками составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.
16	ПСК-1.1 способность участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах (ПСК-1.1);	Знать и понимать: понятия информационной безопасности, типы угроз, методы защиты, составные элементы подсистем и их характеристики, правила эксплуатации используемых подсистем информационной безопасности. Уметь: проводить анализ угроз информационной безопасности, строить политику безопасности, политику управления доступом и информационными потоками в компьютерных системах на основании. Владеть: навыками разработки формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах на основе анализа информационной инфраструктуры.
17	ПСК-1.2 способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований (ПСК 1.2);	Знать и понимать: основные принципы аналитического представления информации и математические законы, позволяющие их обрабатывать. Уметь: применять математические методы синтеза, строить модели защиты с заданными параметрами и анализировать их реакцию на синтезированные внешние воздействия. Владеть: навыками интерпретации полученных описания результатов и формулированию выводов о результатах экспериментов, корректности и эффективности использования необходимых средств защиты.
18	ПСК-1.3 способность выполнять работу по самостоятельному построению алгоритмов,	Знать и понимать: порядок и правила построения алгоритмов, методы проведения их анализа Уметь: формализовывать задачи и данные для их

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	проведению их анализа и реализации в современных программных комплексах (ПСК-1.3);	алгоритмизации и реализации в современных программных комплексах. Владеть: навыками построения алгоритмов, проведения их анализа и реализации в современных программных комплексах.
19	ПСК-1.4 способность проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей (ПСК-1.4);	Знать и понимать: эксплуатационные параметры и технические характеристики аппаратных и технических средств защиты информации. Уметь: проводить экспериментальное исследование работоспособности как отдельных элементов системы защиты, так и компьютерных систем с помощью необходимых технических средств с целью выявления уязвимостей. Владеть: навыками интерпретировать полученные результаты для получения оценки эффективности системы защиты компьютерных систем.

7. Объем, структура и содержание практики, формы отчетности

Общая трудоемкость практики составляет 3 зачетных единиц, 2 недели / 108 часов.

Содержание практики, структурированное по разделам (этапам)

№ п/п	Разделы (этапы) практики	Виды деятельности студентов в ходе практики, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля
		Зет	Часов			
			Все-го	Практичес-кая работа	Самостоятельная работа	
1	2	3	4	5	6	7
1.	Раздел: Организационно-подготовительный этап Обсуждение организационных вопросов с руководителем практики и разработка плана практики.Инструктаж по технике безопасности	0,11	4	4	0	устный опрос
2.	Раздел: Производственный Сбор практического материала по теме ВКР и выполнение индивидуальных заданий руководителя практики;- Обработка собранных материалов, написание первой главы ВКР	2	72	72	0	Промежуточная проверка правильности оформления отчетных материалов
3.	Раздел: Заключительный этап Подготовка отчета и	0,89	32	32	0	- отчет по

№ п/п	Разделы (этапы) практики	Виды деятельности студентов в ходе практики, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля
		Зет	Часов			
			Все-го	Практичес-кая работа	Самостоятельная работа	
1	2	3	4	5	6	7
	представление чернового варианта первой главы ВКР на зачет					практике ЗаО
	Всего:		108	108	0	

Форма отчётности: Форма отчетности по практике: отчет

8. Перечень учебной литературы и ресурсов сети "интернет", необходимых для проведения практики

8.1. Основная литература

№ п\п	Наименование	Авторы	Год и место издания. Место доступа	Используется при изучении разделов, номера страниц
1.	Дискретная математика: Учебное пособие.УДК 681.3 Ж51	Желенков Б.В., Першеев В.Г.	2008, миит.	http://library.miit.ru/
2.	Дискретная математика:Учебное пособие.	Плотников А.Д.	2008, Минск.: Новое знание.	УДК 519.8УДК 519.854(075.8)ISBN 978-985-475-371-3
3.	Схемотехника ЭВМ. Основы построения логических элементов.	Желенков Б.В.	2013, миит.	http://Учебное пособие.УДК 681.3 Ж51library.miit.ru/
4.	Исследование цифровых схем в лабораторном комплексе с использованием	Богодистова Е. С., Долгов И. С., Желенков Б. В.	2012, миит.	Учебное пособие. УДК 681.3 Б74

8.2. Дополнительная литература

№ п\п	Наименование	Авторы	Год и место издания. Место доступа	Используется при изучении разделов, номера страниц
1.	Основы построения опорных сетей ISP.	Желенков Б.В.	2009, миит.	Учебное пособие. УДК 681.3 Ж51http://library.miit.ru/
2.	Проектирование кампусных сетей: Учебное пособие.	Голдовский Я.М.	0.	УДК 681.3 Г60http://library.miit.ru/
3.	Криптографическая защита компьютерной информации. Методические указания к лабораторным работам.	Сафонова И.Е.Голдовский Я.М. Желенков Б.В.	2013, миит.	УДК 681.3 Г60

8.3. Ресурсы сети "Интернет"

1. Электронно-библиотечная система Научно-технической библиотеки МИИТ - http://library.miit.ru/
2. Форум специалистов по информационным технологиям http://citforum.ru/
3. Интернет-университет информационных технологий http://www.intuit.ru/
4. Тематический форум по информационным технологиям http://habrahabr.ru/

9. Образовательные технологии

• мультимедийные технологии для вводной лекций
• презентации
• дистанционная форма групповых и индивидуальных консультаций во время вводной лекций, периода прохождения практики и подготовки отчета

В процессе прохождения практики руководителем от кафедры и руководителем от профильной организации могут применяться современные образовательные технологии, такие как (при необходимости):
- Мультимедийные и дистанционные курсы лекций, системы автоматической проверки знаний, программные симуляторы, системы поддержки видеоконференций;
- электронная форма обмена материалами, а также дистанционная форма групповых и индивидуальных консультаций во время прохождения практики и подготовки отчета;
- использование компьютерных технологий и программных продуктов, необходимых для сбора и систематизации информации, проведения требуемых программой расчетов и т.д.

10. Перечень информационных технологий, программного обеспечения и информационных справочных систем, используемых при проведении практики

Microsoft Windows
Microsoft Office
Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014
Для организации дистанционной работы необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».
При проведении практики может понадобиться наличие следующего программного обеспечения (или их аналогов) – ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.
В образовательном процессе могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

11. Материально-техническая база, необходимая для проведения практики

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

№1329
Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран проекционный Аудитория подключена к интернету МИИТ.
В случае прохождения практики с применением электронного обучения и дистанционных образовательных технологий на базе Университета и его структурных подразделений, или профильного предприятия необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения руководителей практики со студентами, посредством используемых средств коммуникации.