

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:	2019

Одобрено на заседании
Учебно-методической комиссии

Протокол № 2
«30» сентября 2019 г.

Председатель учебно-методической
комиссии  Н.А. Клычева

Одобрено на заседании кафедры

Протокол № 2/а
«27» сентября 2019 г.

Заведующий кафедрой  Б.В. Желенков

Рабочая программа практики в виде электронного
документа выгружена из единой корпоративной
информационной системы управления университетом и
соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 4196
Подписал: Заведующий кафедрой Желенков Борис
Владимирович
Дата: 27.09.2019

1. Цели практики

Преддипломная практика предшествует 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 относится к вариативной части модуля Б2.

Для прохождения преддипломной практики 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 4-ом 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	ПКО-1 Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	ПКО-1.1 Знать порядок обслуживания криптографических средств защиты информации. ПКО-1.2 Уметь обслуживать технические средств защиты информации. ПКО-1.3 Владеть навыками эксплуатации программно-аппаратных и технических средств защиты информации.

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
2	ПКО-2 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;	ПКО-2.1 Знать методы и средства разработки программного обеспечения. ПКО-2.2 Уметь оценивать средства разработки программ. ПКО-2.3 Владеть методами программирования на языках высокого уровня для решения профессиональных задач.
3	ПКО-3 Способность администрировать подсистемы информационной безопасности объекта защиты;	ПКО-3.1 Угрозы безопасности, режимы противодействия. ПКО-3.2 Уметь определять состав и порядок администрирования подсистемы информационной безопасности. ПКО-3.3 Владеть навыками мониторинга функционирования подсистемы ИБ.
4	ПКО-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;	ПКО-4.1 Знать виды комплексного подхода в организации политики информационной безопасности. ПКО-4.2 Уметь формулировать, настраивать политики безопасности. ПКО-4.3 Владеть навыками формулирования и контролирования соблюдения требований политики безопасности.
5	ПКО-5 Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;	ПКО-5.1 Знать нормативную документацию по аттестации объектов информатизации. ПКО-5.2 Уметь выполнять требования безопасности хранения и обработки информации. ПКО-5.3 Владеть навыками аттестации объектов информации по средствам требований информатизации.
6	ПКО-6 Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;	ПКО-6.1 Знать методы и принципы проведения аудита информационной безопасности. ПКО-6.2 Уметь организовывать и проводить аудит работоспособности и эффективности применяемых средств защиты информации. ПКО-6.3 Владеть навыками оценивания оптимальности выбора программно-аппаратных средств защиты информации.
7	ПКО-7 Способность проводить проектные расчеты элементов систем обеспечения информационной безопасности;	ПКО-7.1 Знать методы проведения расчетов и элементы систем обеспечения информационной безопасности. ПКО-7.2 Уметь выбирать необходимые методы для проведения расчета элементов систем обеспечения информационной безопасности. ПКО-7.3 Владеть навыками проведения проектных расчетов элементов систем обеспечения информационной безопасности.
8	ПКО-8 Способность оформлять	ПКО-8.1 Знать действующие нормативные и методические документы.

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	рабочую техническую документацию с учетом действующих нормативных и методических документов;	ПКО-8.2 Уметь анализировать, систематизировать, оформлять техническую документацию. ПКО-8.3 Владеть навыками грамотного составления технической документации.
9	ПКО-9 Способность проводить сбор, изучение научно-технической информации, отечественного и зарубежного опыта по вопросам обеспечения информационной безопасности;	ПКО-9.1 Знать методы поиска научно-технической информации. ПКО-9.2 Уметь выбирать необходимую информацию в области информационной безопасности из отечественных и зарубежных источников. ПКО-9.3 Владеть навыками изучения научно-технической информации, отечественного и зарубежного опыта по вопросам обеспечения информационной безопасности.
10	ПКО-10 Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;	ПКО-10.1 Знать международные и отечественные стандарты соответствия объектов информационной безопасности. ПКО-10.2 Уметь применять стандарты при анализе на соответствие объектов информационной безопасности. ПКО-10.3 Владеть методами проведения анализа объектов информационной безопасности.
11	ПКО-11 Способность проводить обработку и анализ результатов проведения экспериментов по изучению и тестированию системы обеспечения информационной безопасности или ее отдельных элементов;	ПКО-11.1 Знать методы обработки и анализа результатов проведения экспериментов. ПКО-11.2 Уметь выбирать необходимые методы для обработки и анализа результатов проведения экспериментов. ПКО-11.3 Владеть навыками обработки и анализа результатов проведения экспериментов по изучению и тестированию системы обеспечения информационной безопасности или ее отдельных элементов.
12	ПКО-12 Способность принимать участие в проведении экспериментальных исследований системы защиты информации;	ПКО-12.1 Знать принципы функционирования системы защиты информации. ПКО-12.2 Уметь проводить исследование описывая каждый этап эксперимента и обосновывать полученный результат. ПКО-12.3 Владеть методами анализа процедуры исследования и результата согласно заданным критериям.
13	ПКО-13 Способность осуществлять совершенствование системы управления информационной безопасностью;	ПКО-13.1 Знать тенденции развития угроз информационной безопасности. ПКО-13.2 Уметь анализировать уязвимости системы информационной безопасности. ПКО-13.3 Владеть навыками совершенствования системы управления информационной безопасностью на основе анализа угроз и текущего состояния системы информационной безопасности.
14	ПКО-14 Способность организовывать работу малого коллектива исполнителей в профессиональной деятельности;	ПКО-14.1 Знать принципы работы малых коллективов объединенных единой целью. ПКО-14.2 Уметь применить меры для получения продуктивной работы. ПКО-14.3 Владеть организаторскими навыками правильного распределения времени и ресурсов.
15	ПКР-1	ПКР-1.1 Знать принципы работы и правила

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	Способность эксплуатировать и поддерживать в работоспособном состоянии средства защиты информации;	эксплуатации эксплуатируемых программно-аппаратных средств защиты информации. ПКР-1.2 Уметь конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях. ПКР-1.3 Владеть навыками управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях.
16	ПКР-2 Способность участвовать в разработке политик безопасности, политик управления доступом и информационными потоками в компьютерных сетях;	ПКР-2.1 Знать виды политик управления доступом и информационными потоками в компьютерных сетях. ПКР-2.2 Уметь обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях. ПКР-2.3 Владеть навыками разработки порядка применения программно-аппаратных средств защиты информации в компьютерных сетях.
17	ПКР-3 Способность проводить экспериментальное исследование компьютерных сетей с целью выявления уязвимостей;	ПКР-3.1 Знать источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению. ПКР-3.2 Уметь производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях. ПКР-3.3 Владеть навыками контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях.
18	ПКР-4 Способность осуществлять организационно-правовое обеспечение и управление информационной безопасностью, оценивать угрозы объекта защиты.	ПКР-4.1 Знать нормативные правовые акты в области защиты информации. ПКР-4.2 Уметь оценивать угрозы безопасности информации в компьютерных сетях. ПКР-4.3 Владеть навыками управления средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями.

7. Объем, структура и содержание практики, формы отчетности

Общая трудоемкость практики составляет 6 зачетных единиц, 4 недели / 216 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	Практическая 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	0,11	4	4	0	устный опрос

№ 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	Практическая работа	Самостоятельная работа	
1	2	3	4	5	6	7
	технике безопасности					
2.	Раздел: Производственный Сбор практического материала по теме ВКР и выполнение индивидуальных заданий руководителя практики;- Обработка собранных материалов, написание первой главы ВКР	5	180	180	0	Промежуточная проверка правильности оформления отчетных материалов
3.	Раздел: Заключительный этап Подготовка отчета и представление чернового варианта первой главы ВКР на зачет	0,89	32	32	0	- отчет по практике ЗаО
	Всего:		216	216	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 519.8 УДК 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 Ж51 library.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	Желенков Б.В.	2009, миит.	Учебное пособие. УДК

№ п/п	Наименование	Авторы	Год и место издания. Место доступа	Используется при изучении разделов, номера страниц
	сетей ISP.			681.3 Ж51 http://library.mii.ru/
2.	Проектирование кампусных сетей: Учебное пособие.	Голдовский Я.М.	0.	УДК 681.3 Г60 http://library.mii.ru/
3.	Криптографическая защита компьютерной информации. Методические указания к лабораторным работам.	Сафонова И.Е. Голдовский Я.М. Желенков Б.В.	2013, мии.	УДК 681.3 Г60

8.3. Ресурсы сети "Интернет"

1. Электронно-библиотечная система Научно-технической библиотеки МИИТ - <http://library.mii.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.