

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

«26» июня 2019 г.



Кафедра Управление и защита информации

Автор Клепцов Михаил Яковлевич, д.т.н., профессор

**Аннотация к программе практики**

**Преддипломная практика**

Специальность:	<u>10.05.01 Компьютерная безопасность</u>
Специализация:	<u>Информационная безопасность объектов информатизации на базе компьютерных систем</u>
Квалификация выпускника:	<u>Специалист по защите информации</u>
Форма обучения:	<u>Очная</u>
Год начала обучения:	<u>2019</u>

Одобрено на заседании Учебно-методической комиссии  Протокол № 10 «25» июня 2019 г. Председатель учебно-методической комиссии  С.В. Володин	Одобрено на заседании кафедры  Протокол № 21 «24» июня 2019 г. Заведующий кафедрой  Л.А. Баранов
---	---

- 1. Цели практики**
- 2. Задачи практики**
- 3. Место практики в структуре ОП ВО**
- 4. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения ОП**
- 5. Объем, структура и содержание практики, формы отчетности**

# Аннотация к программе практики

## Преддипломная практика

---

(вид практики)

### 1. Цели практики

Целями преддипломной практики являются получение практических знаний, умений и навыков, необходимых для выполнения выпускной квалификационной работы (дипломного проекта) и для успешной адаптации к рынку труда по данной специальности.

### 2. Задачи практики

Задачами преддипломной практики являются:

- закрепление на практике теоретических знаний, полученных при изучении дисциплин базовой части;
- практическое освоение российских и международных стандартов ИБ в рамках деятельности предприятия и оценка степени их применимости для КС данного предприятия;
- приобретение навыков и опыта в проведении обследования защищенности КС и ее подсистем;
- приобретение навыков проектирования систем защиты информации для объектов информатизации;
- умение разрабатывать, апробировать и внедрять технические решения и механизмы защиты информации для конкретных КС;
- освоение технологий сопровождения программно-технических комплексов систем защиты предприятия или компании.

### 3. Место практики в структуре ОП ВО

Преддипломная практика относится к Блоку 2 «Практики, в том числе научно-исследовательская работа (НИР)» части «Производственная практика».

Преддипломную практику студенты проходят на шестом курсе в семестре "В" в течение 4 недель.

Преддипломная практика базируется на освоении дисциплин профессионального цикла, учебной и производственной практик. Знания и умения, приобретенные в результате освоения этих предшествующих части ОП необходимы для успешного освоения преддипломной практики. Прохождение преддипломной практики необходимо для повышения уровня профессиональной подготовки выпускников, а также на качественное выполнение выпускной квалификационной работы, т.е. дипломного проекта.

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

№ п\п	Код компетенции	Содержание компетенции
1	2	3
1	ПКО-1	Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах
2	ПКО-10	Способен организовать процесс защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
3	ПКО-11	Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации
4	ПКО-12	Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности, проводить мониторинг и анализ эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах
5	ПКО-2	Способен применять математические методы в области компьютерной безопасности
6	ПКО-3	Способен проводить анализ исходных данных и формировать требования к компонентам и методам при проектировании подсистем и средств обеспечения информационной безопасности
7	ПКО-4	Способен участвовать в разработке подсистемы информационной безопасности компьютерной (в том числе автоматизированной) системы включая разработку программно-аппаратных средств защиты информации, защищенных операционных систем, систем управления базами данных, компьютерных сетей, систем антивирусной защиты, средств криптографической защиты информации
8	ПКО-5	Способен участвовать в работах по проектированию и реализации комплексного подхода к обеспечению информационной безопасности объекта защиты
9	ПКО-6	Способен проводить оценку эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
10	ПКО-7	Способен проводить анализ информационной безопасности

№ п/п	Код компетенции	Содержание компетенции
1	2	3
		объектов и систем, принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации
11	ПКО-8	Способен проводить инструментальный мониторинг защищенности компьютерных систем
12	ПКО-9	Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию
13	ПКС-1	Способен разрабатывать модели угроз, формировать требования по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации
14	ПКС-2	Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации
15	ПКС-3	Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации
16	ПКС-4	Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем
17	ПКС-5	Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации

## 5. Объем, структура и содержание практики, формы отчетности

Общая трудоемкость практики составляет 12 зачетных единиц, 8 недель/432 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	Практич ес-кая работа	Самостоя- тельная работа	
1	2	3	4	5	6	7
1.	Этап: Подготовительный	0,33	12	8	4	Собесе

№ п/п	Разделы (этапы) практики	Виды деятельности студентов в ходе практики, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текуще го контро ля
		Зет	Часов			
			Все -го	Практич ес-кая работа	Самостоя те-льная работа	
1	2	3	4	5	6	7
	этап					довани е
2.	Этап: Производственный инструктаж	0,67	24	14	10	Проверка знаний
3.	Этап: Выполнение производственных заданий	7,78	280	220	60	Собесе довани е
4.	Этап: Анализ и обобщение фактического материала для отчета	1,39	50	32	18	Собесе довани е
5.	Этап: Подготовка и оформление отчета по преддипломной практике	1,56	56	42	14	Итогов ый отчет
6.	Этап: Проверка и защита отчета по преддипломной практике	0,28	10	4	6	ЗаО
	Всего:		432	320	112	

Форма отчётности: