

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

«08» сентября 2017 г.

Кафедра: Управление и защита информации
Авторы: Клепцов Михаил Яковлевич, доктор технических наук,
профессор

ПРОГРАММА ПРАКТИКИ

преддипломная практика

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов
информатизации на базе компьютерных систем

Квалификация выпускника: Специалист по защите информации

Форма обучения: Очная

Год начала обучения: 2017

Одобрено на заседании
Учебно-методической комиссии

Протокол № 1
«06» сентября 2017 г.

Председатель учебно-методической
комиссии



С.В. Володин

Одобрено на заседании кафедры

Протокол № 2
«04» сентября 2017 г.

Заведующий кафедрой



Л.А. Баранов

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. Тип практики, формы и способы ее проведения

Вид практики: производственная

Тип практики: преддипломная практика

Форма проведения практики: непрерывная

Способ проведения практики: стационарная; выездная.

Преддипломная практика проводится в соответствии с ФГОС ВО и рабочим учебным планом на 6 курсе в семестре В в течение 8 недель.

Преддипломная практика может быть реализована в двух формах:

- практика по получению профессиональных умений и опыта профессиональной

деятельности;

- практика в форме выполнения научно-исследовательской работы (НИР), которая направлена на проведение научных исследований или выполнение программно-технических разработок.

Преддипломная практика может проводиться как в сторонних организациях, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данной специальности (специализации), так и на базе лабораторий РУТ (МИИТ).

5. Организация и руководство практикой

Организация преддипломной практики направлена на обеспечение непрерывности и последовательности овладения обучающимися профессиональной деятельностью и на сбор исходных данных и других материалов, необходимых для выполнения выпускной квалификационной работы – дипломного проекта. Сроки проведения преддипломной практики установлены в соответствии с учебным планом, календарным учебным графиком и с учетом требований ФГОС ВО.

Преддипломная практика осуществляется на базе сторонних предприятий, осуществляющих деятельность, соответствующих видам профессиональной деятельности, указанным в ФГОС ВО. Преддипломная практика осуществляется непрерывно, т.е. в календарном учебном плане для реализации преддипломной практики выделены недели.

Для руководства преддипломной практикой, проводимой в учреждениях, организациях или компаниях назначаются руководители практики от кафедры и от предприятия.

Руководитель преддипломной практики от кафедры:

- устанавливает связь с руководителем практики от предприятия и совместно с ним составляет рабочий план проведения практики и выбирает тематику индивидуальных заданий;
- несет ответственность совместно с руководителем практики от предприятия за соблюдением сроков практики и ее содержанием;
- оказывает методическую помощь обучающимся при выполнении ими индивидуальных заданий и в подборе исходных данных и других материалов для выпускной квалификационной работы;
- оценивает результаты выполнения программы преддипломной практики.

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 осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по	Знания: источники научно-технической информации, отечественный и зарубежный опыт по выбранной тематике в области компьютерной безопасности; методов и методологий, необходимых при решении задач предметной области Умения: грамотно осуществлять подбор, анализ и обобщение информации; уметь ставить задачи и

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	формулировать цели исследований; использовать в своей профессиональной деятельности нормативные правовые акты Навыки и опыт деятельности: навыки в решении задач, в изучении научно-технической и нормативно-правовой информации в рамках выбранной тематики
2	ПК-2 способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	Знания: современного состояния предмета по выбранной тематике Умения: находить новые и применять известные методы и методологии при решении задач по оценке защищенности информации в компьютерных системах Навыки и опыт деятельности: в использовании методов, составлении научных отчетов, обзоров, по результатам выполнения исследований
3	ПК-3 способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знания: требований отечественных и зарубежных стандартов в области компьютерной безопасности; методик проведения анализа безопасности компьютерных систем Умения: выбирать методику проведения анализа системы; проводить анализ безопасности компьютерных систем по выбранным методикам; выявлять несоответствия действующим стандартам безопасности методикам Навыки и опыт деятельности: в использовании различных методик анализа безопасности компьютерных систем
4	ПК-4 способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знания: требований к разработке математических моделей безопасности компьютерных систем Умения: разрабатывать различные математические модели угроз и систем безопасности компьютерных систем; проводить анализ эффективности разработанной модели Навыки и опыт деятельности: в проведении анализа и разработке математических моделей с использованием современных методик, программно-технических средств моделирования и анализа
5	ПК-5 способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знания: основные принципы построения и конфигурирования программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации Умения: разрабатывать и конфигурировать программно-аппаратные средства защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации с учетом решаемых задач и организационной структуры

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
		<p>объекта защиты, внешних воздействий, вероятных угроз и уровня развития информационных технологий</p> <p>Навыки и опыт деятельности: навыки организации работы, опыт анализа, синтеза и конфигурирования программно-аппаратных средств защиты информации с учетом решаемых задач, организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития информационных технологий</p>
6	<p>ПК-6</p> <p>способностью участвовать в разработке проектной и технической документации</p>	<p>Знания: знать и применять методику научных исследований в обеспечении ИБ КС</p> <p>Умения: разрабатывать проектную и техническую документацию для системы обеспечения ИБ ОИ</p> <p>Навыки и опыт деятельности: навыки обобщения результатов НИР для проектных решений по СОИБ объекта информатизации</p>
7	<p>ПК-7</p> <p>способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем</p>	<p>Знания: основы проектирования систем обеспечения информационной безопасности КС и ее компонентов</p> <p>Умения: определять факторы, воздействующие на информацию в объектах информатизации</p> <p>Навыки и опыт деятельности: навыки использования полученных знаний и умений для проведения работ по созданию системы защиты КС</p>
8	<p>ПК-8</p> <p>способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы</p>	<p>Знания: основные компоненты подсистемы ИБ КС</p> <p>Умения: проводить сбор и анализ исходных данных для разработки подсистемы ИБ</p> <p>Навыки и опыт деятельности: навыками проведения основных работ по созданию подсистемы ИБ КС</p>
9	<p>ПК-9</p> <p>способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы</p>	<p>Знания: порядок аттестации и требования к уровню защищенности компьютерной системы</p> <p>Умения: проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности, с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития информационных технологий, выявлять уязвимости КС, используя при необходимости экспериментальные методы</p> <p>Навыки и опыт деятельности: навыки точной и систематической работы со средствами обеспечения информационной безопасности, опыт планирования и постановки эксперимента с целью выявления уязвимостей</p>
10	<p>ПК-10</p> <p>способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления</p>	<p>Знания: методы и средства оценки эффективности реализации систем защиты информации</p> <p>Умения: настраивать действующие политики безопасности с учетом конфигураторов технических средств и ПО</p> <p>Навыки и опыт деятельности: навыками работы со средствами оценки защищенности КС</p>

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	
11	ПК-11 способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	<p>Знания: методику проведения экспериментально-исследовательских работ в выбранной области исследования; требования при проведении сертификации средств защиты информации</p> <p>Умения: находить и анализировать информацию и основные требования по проведению работ в выбранной области исследования</p> <p>Навыки и опыт деятельности: навыками работы с системами защиты информации в выбранной области исследования</p>
12	ПК-12 способностью проводить инструментальный мониторинг защищенности компьютерных систем	<p>Знания: способы и методики проведения инструментального мониторинга и основные программно-технические средства для проведения мониторинга для выбранной тематики</p> <p>Умения: определять уровень защищенности компьютерных систем, используя различные методики и программно-технические средства для выбранной тематики</p> <p>Навыки и опыт деятельности: навыками работы с программно-техническими средствами мониторинга защищенности КС для выбранной тематики</p>
13	ПК-13 способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности	<p>Знания: принципы взаимодействия в малых коллективах с учетом специфики выбранной темы; роль принятых управленческих решений при работе в сфере защиты информации для выбранной тематики</p> <p>Умения: организовывать работу по защите информации и составлять инструкции по выбранной тематике; осознанно принимать управленческие решения и нести ответственность за их последствия</p> <p>Навыки и опыт деятельности: навыками работы в коллективе; навыками организации работ по обеспечению защиты информации по выбранной тематике</p>
14	ПК-14 способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	<p>Знания: требования и способы организации режима защиты информации</p> <p>Умения: обеспечивать режим защиты информации с выполнением требований безопасности; организовывать режим ограниченного доступа</p> <p>Навыки и опыт деятельности: работы с различными системами обеспечения защиты информации</p>
15	ПК-15 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	<p>Знания: знать и учитывать современные тенденции и подходы по совершенствованию СУИБ КС</p> <p>Умения: разрабатывать технологии предложения по модернизации и развитию СУИБ КС</p> <p>Навыки и опыт деятельности: навыками по модернизации СУИБ КС</p>

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
16	<p>ПК-16</p> <p>способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем</p>	<p>Знания: нормативные правовые акты Российской Федерации, касающиеся информационной безопасности</p> <p>Умения: применять на практике требования по защите информации нормативных правовых актов Российской Федерации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития информационных технологий</p> <p>Навыки и опыт деятельности: навыки организации работы и опыт разработки проектов нормативных правовых актов и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем</p>
17	<p>ПК-17</p> <p>способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение</p>	<p>Знания: основные принципы построения, установки и наладки, а также порядок, правила и очередность тестирования и обслуживания современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение</p> <p>Умения: устанавливать, настраивать, тестировать и обслуживать, используемое на предприятии современное общее и специальное программное обеспечение, включая операционные системы, системы управления базами данных, сетевое программное обеспечение с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития информационных технологий</p> <p>Навыки и опыт деятельности: практический опыт установки, наладки, тестирования и обслуживания современного общего и специального программного обеспечения, используемого на предприятии, включая операционные системы, системы управления базами данных, сетевое программное обеспечение с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития информационных технологий</p>
18	<p>ПК-18</p> <p>способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической</p>	<p>Знания: основные принципы построения, конфигурирования и наладки, а также порядок, правила и очередность тестирования и обслуживания современных программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации</p> <p>Умения: устанавливать, настраивать, тестировать и обслуживать современные программно-аппаратные средства защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты</p>

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	защиты информации	<p>информации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития информационных технологий</p> <p>Навыки и опыт деятельности: опыт установки, наладки, тестирования и обслуживания современных программно-аппаратных средств защиты информации с учетом решаемых задач, организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития информационных технологий</p>
19	<p>ПК-19</p> <p>способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации</p>	<p>Знания: основные принципы организации проверки технического состояния, а также порядок, правила и очередность профилактических осмотров технических средств защиты информации</p> <p>Умения: производить проверки технического состояния и профилактические осмотры реальных технических средств защиты информации, используемых на предприятии, с учетом решаемых задач, организационной структуры объекта защиты, внешних воздействий и вероятных угроз</p> <p>Навыки и опыт деятельности: практический опыт проведения проверки технического состояния и профилактических осмотров реальных технических средств защиты информации, используемых на предприятии, с учетом решаемых задач, организационной структуры объекта защиты, внешних воздействий и вероятных угроз</p>
20	<p>ПК-20</p> <p>способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций</p>	<p>Знания: основные принципы, порядок и правила, организации работы по восстановлению работоспособности и поиску неисправностей средств защиты информации при возникновении нештатных ситуаций</p> <p>Умения: производить работы по восстановлению работоспособности реальных средств защиты информации, используемых на предприятии, при возникновении нештатных ситуаций, с учетом решаемых задач, организационной структуры объекта защиты, внешних воздействий и вероятных угроз</p> <p>Навыки и опыт деятельности: практический опыт по поиску неисправностей и восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций с учетом решаемых задач, организационной структуры объекта защиты, внешних воздействий и вероятных угроз</p>
21	<p>ПСК-8.1</p> <p>способностью разрабатывать модели угроз, формировать требования к обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и</p>	<p>Знания: основные этапы и процессы создания СОИБ КС в защищенном исполнении</p> <p>Умения: разрабатывать проектную документацию на СОИБ КС</p> <p>Навыки и опыт деятельности: навыками разработки моделей угроз и модели нарушителя</p>

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	процессов их проектирования, создания и модернизации	
22	ПСК-8.2 способностью разрабатывать проектные решения систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации	Знания: современные технологии проектных решений при разработке СОИБ КС в защищенном исполнении Умения: разрабатывать проектные решения по созданию СОИБ Навыки и опыт деятельности: навыками практического внедрения проектных решений СОИБ для объектов информатизации
23	ПСК-8.3 способностью проводить анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и систем обеспечения информационной безопасности процессов их проектирования, создания и модернизации	Знания: методы и средства проведения анализа СОИБ ОИ на базе КС Умения: проводить анализ СОИБ ОИ на их соответствие требованиям ИБ Навыки и опыт деятельности: навыками анализа и оценки СОИБ ОИ на основе оценки рисков
24	ПСК-8.4 способностью участвовать в создании системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении	Знания: процессы проектирования, создания и модернизации СОИБ на базе КС в защищенном исполнении Умения: определять факторы воздействия на СОИБ КС в защищенном исполнении Навыки и опыт деятельности: навыками организации работ по созданию СОИБ ОИ
25	ПСК-8.5 способностью разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации	Знания: нормативные правовые акты и руководящие документы, регламентирующие деятельность предприятия по проектированию систем обеспечения ИБ Умения: использовать нормативные акты и руководящие документы, регламентирующие деятельность по защите информации при модернизации систем защиты информации объекта информатизации Навыки и опыт деятельности: навыками работы со стандартами для разработки регламентов ИБ объектов информатизации

7. 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	Практическая работа	Самостоятельная работа	
1	2	3	4	5	6	7
1.	Этап: Подготовительный этап	0,33	12	8	4	Собеседование
2.	Этап: Производственный инструктаж	0,67	24	14	10	Проверка знаний
3.	Этап: Выполнение производственных заданий	7,78	280	220	60	Собеседование
4.	Этап: Анализ и обобщение фактического материала для отчета	1,39	50	32	18	Собеседование
5.	Этап: Подготовка и оформление отчета по преддипломной практике	1,56	56	42	14	Итоговый отчет
6.	Этап: Проверка и защита отчета по преддипломной практике	0,28	10	4	6	ЗаО
	Всего:		432	320	112	

Форма отчётности: Форма отчетности по практике: отчет по преддипломной практике.

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.	Поддержка принятия решений при проектировании систем защиты информации	Бухтояров В.В. и др.	2014, М.: ИНФРА-М.	Все разделы
2.	«Информационная безопасность компьютерных систем и сетей». Учебное пособие	Шаньгин В.Ф.	2014, М.: ИД «Форум».	Все разделы

8.2. Дополнительная литература

№ п/п	Наименование	Авторы	Год и место издания. Место доступа	Используется при изучении разделов, номера страниц
1.	Организационное и техническое обеспечение ИБ. Защита конфиденциальной информации: Учебное пособие	Ишейнов В.Я., Мещатунян М.В.	2014, М.: ИД «Форум».	Все разделы
2.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие для ВУЗов	Девянин П.Н.	2011, М., Горячая линия – Телеком.	Все разделы

8.3. Ресурсы сети "Интернет"

9. Образовательные технологии

В процессе прохождения преддипломной практики, в зависимости от видов выполняемых производственных заданий по информационной безопасности на предприятиях или компаниях рекомендуется использовать следующие научно-исследовательские и научно-производственные технологии:

- технологии компаний CISCO и «Информзащита» в части аппаратных и программно-аппаратных средств защиты информации;
- технология антивирусной защиты систем и сетей;
- технология защиты от утечки информации персональной и конфиденциальной информации КС;
- технологии защиты от хакерских атак компании Safen Soft.

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

Для освоения преддипломной практики целесообразно использовать программное обеспечение «Лаборатории Касперского» (<http://writelist.kaspersy.com>) и программное обеспечение от различных угроз информационной безопасности компании Safen Soft (<http://www.safensoft.ru>), а также базу научно-технической информации ВНИТИ РАН. Кроме того, следующие интернет – ресурсы:
<http://www.itsec.ru> - портал информационная безопасность
<http://www.fstec.ru> – сервер ФСТЭК

11. Материально-техническая база, необходимая для проведения практики

В соответствии с профилем специализации «Информационная безопасность объектов информатизации на базе компьютерных систем» для проведения преддипломной практики необходимо следующее материально-техническое обеспечение:

- лаборатории и специально оборудованные кабинеты кафедры «Управление и защита информации»;

- измерительные и вычислительные комплексы и лаборатории кафедры «Вычислительные системы и сети»;

При прохождении преддипломной практики на предприятии должна быть материально-техническая база, удовлетворяющая специфику направления подготовки специалиста по защите информации.

В процессе прохождения преддипломной практики, при необходимости, может использоваться научная электронная библиотека «Веда» (info@beb.ua-ru.net).