МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

«26» мая 2020 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:	2020

Одобрено на заседании Учебно-методической комиссии	Одобрено на заседании кафедры
Протокол № 10 «26» мая 2020 г. Председатель учебно-методической комиссии _____ С.В. Володин	Протокол № 16 «21» мая 2020 г. Заведующий кафедрой _____ Л.А. Баранов

Москва 2020

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».
Преддипломная 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 проводится 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	ПКО-1 Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские	ПКО-1.1 Участвует в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах. ПКО-1.2 Изучает и анализирует отечественный и зарубежный опыт по проблемам компьютерной безопасности.

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	работы по оценке защищенности информации в компьютерных системах	ПКО-1.3 Участвует в проведении экспериментально-исследовательских работ при сертификации средств защиты информации.
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	ПКО-10.1 Проверяет уровень квалификации, распределяет полномочия и контролирует выполнение инструкций в отношении персонала обслуживающего технические, программные и программно-аппаратные средства защиты информации. ПКО-10.2 Анализирует компьютерные системы в сфере профессиональной деятельности с целью выявления условий, способствующих совершению правонарушений в отношении сведений ограниченного доступа.
3	ПКО-11 Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации	ПКО-11.1 Обосновывает критерии и рассчитывает показатели эффективности защиты обрабатываемой информации. ПКО-11.2 Составляет методики тестирования, подбирает инструментарии? и осуществляет проверку эффективности функционирования программных, программно-аппаратных и технических средств, подсистем защиты информации. ПКО-11.3 Выполняет 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	ПКО-12.1 Выполняет работы, связанные с реализацией частных политик информационной безопасности автоматизированной системы. ПКО-12.2 Проводит мониторинг и аудит безопасности компьютерной системы в сфере профессиональной деятельности. ПКО-12.3 Формирует основные показатели и критерии эффективности, оценивает эффективность компьютерной системы и ее средств защиты в области профессиональной деятельности.
5	ПКО-2 Способен применять математические методы в области компьютерной безопасности	ПКО-2.1 Проводит анализ и разрабатывает под руководством квалифицированного специалиста математические модели безопасности компьютерных систем. ПКО-2.2 Применяет специальные математические методы, включая криптографические, для анализа и разработки защищенных компьютерных систем. ПКО-2.3 Применяет решения на основе специальных математических методов для обеспечения защищенной передачи данных в современных компьютерных сетях.
6	ПКО-3 Способен проводить анализ исходных данных и формировать требования к	ПКО-3.1 Изучает и обобщает опыт работы различных учреждении?, организации? и предприятии? в области повышения эффективности защиты информации. ПКО-3.2 Формирует требования по защите

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	компонентам и методам при проектировании подсистем и средств обеспечения информационной безопасности	информации, включая использование математического аппарата для решения прикладных задач. ПКО-3.3 Составляет планы этапов проведения научно-исследовательских и опытно- конструкторских работ. ПКО-3.4 Разрабатывает и анализирует структурные и функциональные схемы защищенных компьютерных систем в сфере профессиональной деятельности.
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	ПКО-4.1 Осуществляет рациональный выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности, создаваемых защищенных компьютерных систем в сфере профессиональной деятельности. ПКО-4.2 Проектирует и разрабатывает компоненты защищенных автоматизированных систем в сфере профессиональной деятельности.
8	ПКО-5 Способен участвовать в работах по проектированию и реализации комплексного подхода к обеспечению информационной безопасности объекта защиты	ПКО-5.1 Принимает участие в формировании политики информационной безопасности, ее реализации и контроле выполнения. ПКО-5.2 Формирует, организует и поддерживает комплекс мер по обеспечению информационной безопасности.
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	ПКО-6.1 Подбирает методики и инструментарий, определяет критерии и осуществляет проверку эффективности 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 объектов и систем, принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия	ПКО-7.1 Проводит анализ безопасности компьютерных систем, в том числе с использованием методов моделирования, на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности. ПКО-7.2 Участвует в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требовании? к уровню защищенности

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	требованиям защиты информации	компьютерной системы. ПКО-7.3 Вырабатывает рекомендации в связи с проведенным анализом безопасности, в том числе для принятия решения о повторной аттестации компьютерной системы (в том числе автоматизированных систем), предложения по устранению выявленных уязвимостей.
11	ПКО-8 Способен проводить инструментальный мониторинг защищенности компьютерных систем	ПКО-8.1 Анализирует защищенность компьютерных систем с использованием сканеров безопасности. ПКО-8.2 Анализирует защищенность сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем.
12	ПКО-9 Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию	ПКО-9.1 Разрабатывает и организует выполнение мероприятий в соответствии с положениями политики информационной безопасности и защиты информации ограниченного доступа. ПКО-9.2 Разрабатывает предложения по совершенствованию системы управления информационной безопасностью компьютерной системы. ПКО-9.3 Разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем.
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	ПКС-1.1 Знать основные формальные модели изолированной программной среды и безопасности информационных потоков. ПКС-1.2 Уметь разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем.
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	ПКС-2.1 Знать основные процессы проектирования систем обеспечения информационной безопасности. ПКС-2.2 Уметь разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.
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	ПКС-3.1 Знать основные методы и подходы к анализу защищенности компьютерных систем. ПКС-3.2 Уметь применять инструментальные средства анализа защищенности компьютерных систем на объектах информатизации. ПКС-3.3 Владеть навыками разработки документации по сопровождению систем обеспечения информационной безопасности на объектах информатизации.
16	ПКС-4	ПКС-4.1 Знать основные принципы и методы создания

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем	системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении. ПКС-4.2 Уметь создавать системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации. ПКС-4.3 Владеть навыками создания систем обеспечения информационной безопасности.
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	ПКС-5.1 Знать основные принципы разработки нормативно правовых актов, руководящих и методических документов предприятия, учреждения, организации. ПКС-5.2 Уметь разрабатывать нормативно правовые акты, руководящие и методические документы, регламентирующие деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования. ПКС-5.3 Владеть навыками разработки нормативной правовой документации.

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	Практичес-кая работа	Самостоя те-льная 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

№ 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	Самостоя те-льная работа	
1	2	3	4	5	6	7
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., Мецатунян М.В.	2014, М.: ИД «Форум».	Все разделы
2.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками:	Девянин П.Н.	2011, М., Горячая линия – Телеком.	Все разделы

№ п\п	Наименование	Авторы	Год и место издания. Место доступа	Используется при изучении разделов, номера страниц
	Учебное пособие для ВУЗов			

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 компанииSafen Soft (http://www.safensoft/.ru), а также базу научно- технической информации ВИНИТИ 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).