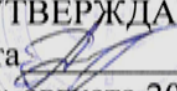


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета  С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

«Преддипломная практика»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2016

Автор программы



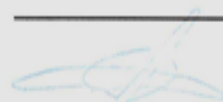
/ А.Г. Остапенко /

Заведующий кафедрой
Систем информационной
безопасности



/ А.Г. Остапенко

Руководитель ОПОП



/ А.Г. Остапенко /

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

1.1. Цели практики

Производственная практика (преддипломная) студентов является заключительной частью образовательного процесса и направлена на закрепление и углубление компетенций, полученных студентами в процессе всего предыдущего обучения, а также на углубление студентом первоначального профессионального опыта, развитие общих и профессиональных компетенций и опытом профессиональной деятельности по получаемой специальности.

1.2. Задачи прохождения практики

- 1) Обобщение и совершенствование знаний и практических навыков, полученных студентами в процессе обучения по специальности;
- 2) Проверка возможностей самостоятельной работы будущего специалиста в условиях конкретного производства;
- 3) Сбор материала для выполнения дипломного проекта;

2. ХАРАКТЕРИСТИКА ПРАКТИКИ

Вид практики – Производственная практика

Тип практики – Преддипломная практика

Форма проведения практики – дискретно

Способ проведения практики – стационарная, выездная.

Стационарная практика проводится в профильных организациях, расположенной на территории г. Воронежа.

Выездная практика проводится в местах проведения практик, расположенных вне г. Воронежа.

Способ проведения практики определяется индивидуально для каждого студента и указывается в приказе на практику.

Место проведения практики – перечень объектов для прохождения практик устанавливается на основе типовых двусторонних договоров между предприятиями (организациями) и ВУЗом или ВУЗ.

3. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП

Практика «Преддипломная практика» относится к базовой части блока Б2.

4. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс прохождения практики «Преддипломная практика» направлен на формирование следующих компетенций:

ОПК-1-способность анализировать физические явления и процессы при решении профессиональных задач

ОПК-2-способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов

ОПК-5-способностью использовать нормативные правовые акты в своей профессиональной деятельности

ОПК-7-способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения

ОПК-9-способностью разрабатывать формальные модели политик безопасности, политику управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации

ПК-3-способностью проводить анализ безопасности компьютерных систем в соответствии с отечественными и зарубежными стандартами в области компьютерной безопасности

ПК-4-способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем

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

ПК-7-способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем

ПК-14-способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа

ПСК-3.1-способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем

ПСК-3.2-способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем

ПСК-3.3-способностью использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности

ПСК-3.4-способностью организовывать защиту информации в распределенных компьютерных системах

ПСК-3.5-способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-1	Знать теоретические основы и задачи физики и математики в контексте обеспечения компьютерной безопасности
	Уметь определять возможности применения на практике физико-математических теоретических положений и методов для постановки и решения прикладных задач по защите информации
	Владеть моделями и методиками

	физико-математического моделирования процессов нарушения компьютерной безопасности
ОПК-2	Знать теоретические основы алгебры, геометрии, математического анализа, теории вероятности, математической статистики, математической логики, теории алгоритмов, теории информации в контексте обеспечения компьютерной безопасности
	Уметь применять на практике математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятности, математической статистики, теории алгоритмов, теории информации для решения практических задач в контексте компьютерной безопасности
	Владеть методами математического исследования процессов нарушения компьютерной безопасности
ОПК-5	Знать методы научных исследований в профессиональной деятельности
	Уметь применять теоретическую базу для проектирования программного обеспечения и устройств
	Владеть навыками и методами создания программного обеспечения и устройств для решения профессиональных задач
ОПК-7	Знать методы техники безопасности при работе с приборами и оборудованием для защиты информации
	Уметь применять на практике работу с офисной техникой
	использовать специализированное оборудование с учетом требований техники безопасности
	Владеть навыками работы с измерительными приборами и типовым оборудованием для защиты информации
ОПК-9	Знать методы разработки формальных моделей политик безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации
	Уметь применять на практике работу с моделями политик безопасности, управления доступом и информационными потоками
	Владеть навыками работы с моделями политик безопасности, управления доступом и информационными потоками
ПК-3	Знать теоретические и практические основы средств обеспечения компьютерной безопасности данных

	Уметь применять на практике основные законы и нормативные документы в области компьютерной безопасности
	Владеть навыками анализа основных узлов устройств современных компьютерных систем
ПК-4	Знать теоретические основы моделирования угроз и нарушителей компьютерной безопасности
	Уметь разрабатывать модели угроз и нарушителей компьютерной безопасности
	Владеть приемами практического применения моделей угроз и нарушителей компьютерной безопасности
ПК-5	Знать теоретические основы конфигурирования программно-аппаратных средств защиты информации
	Уметь применять на практике политику обеспечения компьютерной безопасности
	Владеть навыками защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
ПК-7	Знать основы работы с научно-технической документацией
	Уметь готовить научно-технические отчеты, обзоры и публикации по результатам выполненных работ
	Владеть навыками компьютерной работы с научно-технической документацией, публикацией статей и монографий
ПК-14	Знать теоретические и практические основы организации работы по выполнению режима защиты информации, в том числе ограниченного доступа
	Уметь участвовать в контрольных проверках работоспособности применяемых программно-аппаратных средств для обеспечения компьютерной безопасности
	Владеть навыками, приемами защиты информации и основами организации работы по выполнению режима защиты информации
ПСК-3.1	Знать теоретические основы анализа безопасности распределенных компьютерных систем
	Уметь применять на практике профессиональные навыки в сфере анализа безопасности распределенных компьютерных систем

	стем Владеть современными критериями и стандартами для анализа безопасности распределенных компьютерных систем
ПСК-3.2	Знать теоретические основы в сфере защиты информации распределенных компьютерных систем Уметь применять на практике анализ защиты информации в распределенных компьютерных системах Владеть навыками мониторинга, аудита и контрольных проверок работоспособности и защищенности распределенных компьютерных систем
ПСК-3.3	Знать теоретические основы в сфере защиты информации распределенных компьютерных систем Уметь применять на практике защиту информации в распределенных компьютерных системах Владеть навыками обеспечения защиты информации в распределенных компьютерных системах
ПСК-3.4	Знать организационные навыки защиты информации в распределенных компьютерных системах Уметь организовывать защиту информации в распределенных компьютерных системах Владеть навыками обеспечения профессиональной организации защиты информации в распределенных компьютерных системах
ПСК-3.5	Знать теоретические основы политики информационной безопасности распределенных компьютерных систем Уметь применять на практике формирование, реализацию и контроль эффективности политики информационной безопасности распределенных компьютерных систем Владеть способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем

5. ОБЪЕМ ПРАКТИКИ

Общий объем практики составляет 213 е.е., ее продолжительность – 14 недель.

Форма промежуточной аттестации: зачет с оценкой.

6. СОДЕРЖАНИЕ ПРАКТИКИ

6.1 Содержание разделов практики и распределение трудоемкости по этапам

№ п/п	Наименование этапа	Содержание этапа	Трудоемкость, час
1	Подготовительный этап	Проведение собрания по организации практики. Знакомство с целями, задачами, требованиями к практике и формой отчетности. Распределение заданий. Инструктаж по охране труда и пожарной безопасности.	2
2	Знакомство с ведущей организацией	Изучение организационной структуры организации. Изучение нормативно-технической документации.	10
3	Практическая работа	Выполнение индивидуальных заданий. Сбор практического материала.	732
4	Подготовка отчета	Обработка материалов практики, подбор и структурирование материала для раскрытия соответствующих тем для отчета. Оформление отчета. Предоставление отчета руководителю.	10
5	Защита отчета		2
Итого			756

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

7.1 Подготовка отчета о прохождении практики

Аттестация по итогам практики проводится в виде зачета с оценкой на основе экспертной оценки деятельности обучающегося за защиту отчета. По завершении практики студенты в последний день практики представляют на выпускающую кафедру: дневник практики, включающий всебя отзывы руководителей практики от предприятия и ВУЗа, разработку студента в период практики с оценкой уровня оперативности выполнения им задания по практике, отношения к выполнению программ по практике и т.п.; отчет по практике, включающий текстовые, табличные и графические материалы, отражающие решение предусмотренных заданием на практику задач. В отчете приводится анализ поставленных задач; выбор необходимых методов и инструментальных средств для решения поставленных задач; результаты решения задач практики; общие выводы по практике. Типовая структура отчета:

1. Титульный лист
2. Содержание
3. Введение (цель практики, задачи практики)
4. Практические результаты прохождения практики
5. Заключение
6. Списки использованных источников литературы
7. Приложения (при наличии)

7.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 11 семестре для очной формы обучения по четырем балльной системе:

- «отлично»;
- «хорошо»;

«удовлетворительно»;
«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Экспертная оценка результатов	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-1	Знать теоретические основы и задачи физики и математики в контексте обеспечения компьютерной безопасности	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено	Более 80% от максимального возможного количества баллов	61%-80% от максимального возможного количества баллов	41%-60% от максимального возможного количества баллов	Менее 41% от максимального возможного количества баллов
	Уметь определять возможности применения на практике физико-математических теоретических положений и методов для постановки и решения прикладных задач по защите информации	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть моделями и методиками физико-математического моделирования процессов нарушения компьютерной безопасности	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ОПК-2	Знать теоретические основы алгебры, геометрии, математического анализа, теории вероятности, математической статистики, математической логики, теории алгоритмов, теории информации в контексте обеспечения компьютерной безопасности	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять на практике математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятности, математической статистики, теории алгоритмов, теории информации для решения практических задач в контексте компьютерной безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть методами математического исследования процессов	2 - полное приобретение владения 1 – неполное приобретение				

	нарушения компьютерной безопасности	владения 0 – владениенеприобретено				
ОПК-5	Знать методы научных исследований в профессиональной деятельности	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять теоретическую базу для проектирования программного обеспечения и устройств	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками и методами создания программного обеспечения и устройств для решения профессиональных задач	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ОПК-7	Знать методы техники безопасности при работе с приборами и оборудованием для защиты информации	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять на практике работу с офисной техникой и специализированным оборудованием с учетом требований техники безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками работы с измерительными приборами и типовым оборудованием для защиты информации	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ОПК-9	Знать методы разработки формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять на практике работу с моделями политик безопасности, управления доступом и информационными потоками	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками работы с моделями политик безопасности, управления доступом и информационными потоками	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПК-3	Знать теоретические и практические основы	2 - полное освоение знания 1 – неполное освоение				

	средств обеспечения компьютерной безопасности данных	знания 0 – знание не освоено				
	Уметь применять на практике основные законы и нормативные документы в области компьютерной безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками анализа основных узлов устройств современных компьютерных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-4	Знать теоретические основы моделирования угроз и нарушителей компьютерной безопасности	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь разрабатывать модели угроз и нарушителей компьютерной безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть приемами практического применения моделей угроз и нарушителей компьютерной безопасности	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-5	Знать теоретические основы конфигурирования программно-аппаратных средств защиты информации	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять на практике политику обеспечения компьютерной безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-7	Знать основы работы с научно-технической документацией	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь готовить научно-технические отчеты, обзоры и публикации по результатам выполненных работ	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				

	Владеть навыками компьютерной работы с научно-технической документацией, публикацией статей и монографий	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПК-1 4	Знать теоретические и практические основы организации работы по выполнению режима защиты информации, в том числе ограниченного доступа	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь участвовать в контрольных проверках работоспособности применяемых программно-аппаратных средств для обеспечения компьютерной безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками, приемами защиты информации и основами организации работы по выполнению режима защиты информации	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПСК -3.1	Знать теоретические основы анализа безопасности распределенных компьютерных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять на практике профессиональные навыки в сфере анализа безопасности распределенных компьютерных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть современными критериями и стандартами для анализа безопасности распределенных компьютерных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПСК -3.2	Знать теоретические основы в сфере защиты информации распределенных компьютерных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять на практике анализ защиты информации в распределенных компьютерных системах	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками мониторинга, аудита и контрольных проверок работоспособности и защищенности распределенных компьютерных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				

ПСК -3.3	Знать теоретические основы в сфере защиты информации распределенных компьютерных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять на практике защиту информации в распределенных компьютерных системах	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками обеспечения защиты информации в распределенных компьютерных системах	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПСК -3.4	Знать организационные навыки защиты информации в распределенных компьютерных системах	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь организовывать защиту информации в распределенных компьютерных системах	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками обеспечения профессиональной организации защиты информации в распределенных компьютерных системах	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПСК -3.5	Знать теоретические основы политики информационной безопасности распределенных компьютерных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять на практике формирование, реализацию и контроль эффективности политики информационной безопасности распределенных компьютерных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				

Экспертная оценка результатов освоения компетенций производится руководителем практики (или согласованная оценка руководителя практики от ВУЗа и руководителя практики от организации).

8УЧЕБНО-МЕТОДИЧЕСКОЕИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕПРАКТИКИ

8.1Переченьучебнойлитературы,необходимойдляосвоенияпрактик

и

Основная литература

1.Эпидемии в телекоммуникационных сетях [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 282 с. : ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN 978-5-9912-0682-2 : 736-00.

2.Социальные сети и деструктивный контент [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 274 с. : ил. - (Теория сетевых войн. № 3). - Библиогр.: с. 224-239 (278 назв.). - ISBN 978-5-9912-0686-0 : 719-00.

3.Атакуемые взвешенные сети [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 247 с. : ил. - (Теория сетевых войн. № 2). - Библиогр.: с. 201-213 (214 назв.). - ISBN 978-5-9912-0684-6 : 708-00.

Дополнительная литература

1. Теория сетевых войн [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (894 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00.

2. Сетевое противоборство социотехнических систем [Электронный ресурс] . - Электрон. текстовые, граф. дан. (474Кб). - Воронеж : ФГБОУ ВПО "Воронежскийгосударственныйтехническийуниверситет", 2015. - 1 файл. - 30-00.

3. Информационные технологии и системы государственного и муниципального управления [Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл : 3164 Кб). - Воронеж : ГОУВПО "Воронежскийгосударственныйтехническийуниверситет", 2007. - 1 файл. - 30-00.

8.2Переченьресурсовсети"Интернет",необходимыхдляпроведения практики

<http://att.nica.ru>
<http://www.edu.ru/>
<http://window.edu.ru/window/library>
<http://www.intuit.ru/catalog/>
<https://marsohod.org/howtostart/marsohod2>
<http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp>
<https://cchgeu.ru/education/cafedras/kafsib/?docs>
<http://www.eios.vorstu.ru>
<http://e.lanbook.com/> (ЭБС Лань)
<http://IPRbookshop.ru/> (ЭБСИPRbooks)

8.3Переченьинформационныхтехнологий,используемыхприосущес

твлении образовательного процесса по практике, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

1. Microsoft Office Excel 2013/2007 (Контракт №72, 12.12.2014)
2. Microsoft Office Word 2013/2007 (Контракт №72, 12.12.2014)
3. Интегрированная среда разработки для языка программирования R (GNU GPLv2)
4. Программный комплекс «Netepidemic» для риск-анализа процессов распространения деструктивного контента в неоднородных сетевых структурах.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.