

**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

«Практика по получению профессиональных умений и опыта
профессиональной деятельности»

Специальность 10.05.01 «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»

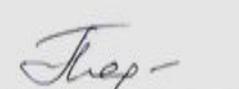
Специализация «Безопасность распределенных компьютерных систем»

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы  /Поздышева О.В./

**Заведующий кафедрой
Систем информационной
безопасности**  /А.Г. Остапенко/

Руководитель ОПОП  /А.Г. Остапенко/

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины - закрепление, дополнение и углубление теоретических знаний, полученных студентами при изучении общетехнических и специальных дисциплин учебного плана.

1.2. Задачи освоения дисциплины

- выявить умение студента применить полученные знания на практике;
- развитие навыков познавательной деятельности, ведения самостоятельной работы по проектированию и изготовлению изделий, овладение методикой исследования, экспериментирования и оформления документации;
- ознакомление с задачами предприятия (организации) и отрасли по повышению эффективности производства, внедрению новейших достижений науки и техники;
- ознакомление с технической и технологической документацией, с патентно-технической литературой;
- изучение мероприятий по охране труда, охране окружающей среды, гражданской обороне.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина Б2.П.3 «Практика по получению профессиональных умений и опыта профессиональной деятельности» относится к дисциплинам блока Б2.П «Производственная практика».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПОД ДИСЦИПЛИНЕ

Процесс изучения дисциплины Б2.П.3 «Практика по получению профессиональных умений и опыта профессиональной деятельности» направлен на формирование следующих компетенций:

Компетенция	Результаты обучения, характеризующие сформированность компетенции
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
	Знать: - основные понятия в сфере профессиональной

	<p>деятельности.</p> <p>Уметь: - осуществлять поиск необходимой информации в открытых научно-технических источниках.</p> <p>Владеть: - методами патентного поиска информации.</p>
ПК-3	<p>способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности</p> <p>Знать: - отечественные и зарубежные стандарты в области компьютерной безопасности.</p> <p>Уметь: - проводить анализ рисков информационной безопасности компьютерной системы.</p> <p>Владеть: - навыками анализа безопасности компьютерных систем.</p>
ПК-5	<p>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</p> <p>Знать: - возможности и основные параметры конфигурирования существующих компьютерных систем.</p> <p>Уметь: - проводить анализ технических и эксплуатационных параметров компьютерных систем.</p> <p>Владеть: - навыками программирования систем защиты компьютерных систем и устройств.</p>
ПК-6	<p>способностью участвовать в разработке проектной и технической документации</p> <p>Знать: - существующие модели угроз информационной безопасности.</p> <p>Уметь: - оценивать технические возможности и выработать рекомендации по построению систем защиты.</p> <p>Владеть: - методами моделирования работы систем безопасности.</p>
ПК-8	<p>способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы</p> <p>Знать: - методы и средства обнаружения уязвимостей автоматизированной системы.</p> <p>Уметь: - разрабатывать эффективные алгоритмы и программы защиты информации.</p>

	<p>Владеть: - навыками безопасного использования программно-аппаратных средств в системах защиты информации.</p>
ПК-12	способностью проводить инструментальный мониторинг защищенности компьютерных систем
	<p>Знать: - методы и средства противодействия атакам на ресурсы компьютерной системы.</p>
	<p>Уметь: - производить анализ и защиту от атак на ресурсы компьютерной системы.</p>
	<p>Владеть: - методикой контроля информационной целостности компьютерной системы.</p>
ПК-13	способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности
	<p>Знать: - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.</p>
	<p>Уметь: - осуществлять рациональный выбор средств и методов защиты информации в компьютерных системах.</p>
	<p>Владеть: - методиками анализа результатов работы обнаружения вторжений.</p>
ПК-17	способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение
	<p>Знать: - современные средства и методы мониторинга, технической диагностики средств защиты.</p>
	<p>Уметь: - выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности компьютерных систем.</p>
	<p>Владеть: - средствами борьбы с атаками злоумышленников на технические и программно-аппаратные средства защиты компьютерных систем.</p>
ПК-18	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

	<p>антивирусной защиты, средства криптографической защиты информации</p> <p>Знать: - физическую организацию баз данных и принципы (основы) их защиты.</p> <p>Уметь: - разрабатывать эффективные процедуры и методы для защиты информации ограниченного доступа.</p> <p>Владеть: - методиками анализа результатов работы обнаружения вторжений.</p>
ПК-19	<p>способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации</p> <p>Знать: - современные средства и методы мониторинга, технической диагностики средств защиты, оценки эффективности информационной безопасности компьютерных систем.</p> <p>Уметь: - выбирать необходимые инструментальные средства анализа защищенности компьютерных системах.</p> <p>Владеть: - средствами борьбы с атаками злоумышленников на ресурсы серверов баз данных.</p>
ПК-20	<p>способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций</p> <p>Знать: - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.</p> <p>Уметь: - осуществлять рациональный выбор средств и методов защиты информации в компьютерных системах.</p> <p>Владеть: - методами расчета и инструментального контроля показателей технической защищенности информации.</p>

4. ОБЪЕМ ДИСЦИПЛИНЫ

Виды учебной работы	Всего часов	Семестры
		4
Самостоятельная работа	108	108
Виды промежуточной аттестации – зачет с оценкой	+	+
Общая трудоемкость час	108	108
з.е.	3	3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Формы проведения производственной практики

Производственная практика проводится в форме научно-исследовательской практики на базовых предприятиях кафедры, на базе Регионального учебно-научного центра по проблемам информационной безопасности и кафедры систем информационной безопасности. Форма проведения производственной практики может быть стационарной или выездной (в другие города РФ).

Общее методическое руководство практикой и непосредственное руководство осуществляет преподаватель, утвержденный приказом ректора или проректора по учебной работе.

Руководство практикой студентов в структурном подразделении – базе практики – возлагается на специалистов указанных подразделений. Руководитель практики от организации осуществляет повседневное организационно-методическое руководство и контроль хода практики закрепленного за ним студента и определяет ему конкретное задание, помогает в сборе необходимых материалов.

Основными нормативно-методическими документами, регламентирующими работу студентов на практике, являются программа практики, а также методические указания руководителя практики от ВГТУ.

5.2 Место и время проведения производственной практики

Продолжительность производственной практики в 4 семестре: 2 недели.

Студенты проходят практику на договорной основе.

Базы практики - предприятия, с которыми были заключены договоры, а также – выпускающая кафедра.

5.3. Трудоемкость производственной практики

Общая трудоемкость производственной практики составляет 3 зачётных единицы, 108 часов.

5.4. Порядок проведения

Перед прохождением практики студент должен получить направление на практику ответственного лица кафедры, изучить программу и обратиться к соответствующим нормативным материалам с тем, чтобы быть подготовленным к выполнению поручений, данных руководителем практики, решению конкретных вопросов.

До начала практики необходимо уточнить на кафедре сроки проведения практики; у руководителя практики получить программу практики, дневник, указания по выполнению индивидуального задания, информацию о графике консультаций и т. п. Выяснить дату проведения зачёта по практике и сроки представления отчётной документации.

Приступить к работе в соответствии со сроками практики и календарным графиком её проведения.

Во время прохождения практики строго соблюдать правила внутреннего трудового распорядка, выполнять все указания руководителей практики. В полном объёме выполнить программу практики и индивидуальное задание.

В случае серьезных нарушений правил внутреннего трудового распорядка, требований техники безопасности студент может быть отстранён от практики.

По окончании практики руководитель практики от кафедры составляет краткий отзыв о каждом студенте, проходившем практику на данной базе практики. Студенты в процессе прохождения практики составляют дневник практики, а по окончании практики – отчет. С разрешения руководителя практики студент оставляет у себя составленные им проекты электронных документов.

Производственную практику студент совместно с преподавателем и руководителем практики может использовать как подготовку к выбору комплексного индивидуального задания, каждый этап выполнения которого на третьем, четвёртом и пятом курсах будет включен в реальный дипломный проект.

6. Темы индивидуальных заданий

Производственная практика ориентирована на ознакомление и приобретение навыков в одном (или нескольких взаимосвязанных) из ниже перечисленных вопросов:

1. Изучение организационного строения базовых предприятий (организаций), назначения отдельных подразделений и служб, а также их взаимодействия.

2. Изучение используемых в структуре предприятия методов и средств защиты информации, а также оборудования, предназначенного для этих целей.

3. Проектирование систем управления информационной безопасностью автоматизированных систем.

4. Подбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности автоматизированных систем с целью выбора оптимального варианта.

5. Ознакомление с методами и соответствующим оборудованием для производства и контроля годности аппаратуры. Приобретение практических навыков работы с оборудованием для контроля и локализации инцидентов/призрачные информации.

6. Разработка программных и аппаратных комплексов защиты информации автоматизированных систем.

7. Изучение структуры, состава программно-аппаратных средств защиты информации и информационных систем.

8. Изучение и практическое применение новых информационных технологий для решения разнообразных прикладных задач и разработки специализированных комплексов защиты информации.

9. Патентно-информационное исследование по выбору вариантов возможных решений по теме и их оценке, сопоставление с техническим уровнем современных отечественных и зарубежных аналогов.

10. Разработка и оформление рабочих чертежей и другой технической и эксплуатационной документации на спроектированное изделие или программные средства.

11. Определение эффективности разработанных методов и качества составленных программ.

12. Анализ технологического процесса как объекта управления, разработка модели объекта и создание политик информационной безопасности конкретных автоматизированных систем.

13. Техническое проектирование средств защиты информации.

14. Разработка отдельных подсистем защиты информации.

15. Программная реализация перспективных методов защиты информации в автоматизированных системах.

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 4 семестре по четырехбальной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл	Неудовл
ПК-2	Знать: - основные понятия в сфере профессиональной деятельности.	знание и использование учебного материала в процессе выполнения заданий по практике	Задание по практике выполнено в полном объеме. Студент	Студент демонстрирует значительное понимание материала.	Студент демонстрирует частичное понимание материала.	1. Задание по практике выполнено не полностью.
	Уметь: - осуществлять поиск необходимой информации в открытых научно-технических источниках.	умение находить и использовать информационный ресурс в процессе выполнения заданий по практике	демонстрирует ярко выраженную способность	Студент демонстрирует способность использовать	Способность студента продемонстрировать знание, умение,	2. Студент демонстрирует непонимание заданий. 3. Студент не смог ответить

	Владеть: - методами патентного поиска информации.	решение практических задач в конкретной предметной области	использовать знания, умения, навыки в процессе выполнения заданий	ать знания, умения, навыки в процессе выполнения заданий	навык выражена слабо	на поставленные вопросы. 4. Не было попытки выполнить задание.
ПК-3	Знать: - отечественные и зарубежные стандарты в области компьютерной безопасности.	знание и использование учебного материала в процессе выполнения заданий по практике				
	Уметь: - проводить анализ рисков информационной безопасности компьютерной системы.	умение находить и использовать информационный ресурс в процессе выполнения заданий по практике				
	Владеть: - навыками анализа безопасности компьютерных систем.	решение практических задач в конкретной предметной области				
ПК-5	Знать: - возможности и основные параметры конфигурирования существующих компьютерных систем.	знание и использование учебного материала в процессе выполнения заданий по практике				
	Уметь: - проводить анализ технических и эксплуатационных параметров компьютерных систем.	умение находить и использовать информационный ресурс в процессе выполнения заданий по практике				
	Владеть: - навыками программирования систем защиты компьютерных систем и устройств.	решение практических задач в конкретной предметной области				
ПК-6	Знать: - существующие модели угроз информационной безопасности.	знание и использование учебного материала в процессе выполнения заданий по практике				
	Уметь: - оценивать технические возможности и выработать рекомендации по построению систем защиты.	умение находить и использовать информационный ресурс в процессе выполнения заданий по практике				
	Владеть: - методами моделирования работы систем безопасности.	решение практических задач в конкретной предметной области				

ПК-8	Знать: - методы и средства обнаружения уязвимостей компьютерных систем.	знание и использование учебного материала в процессе выполнения заданий по практике				
	Уметь: - разрабатывать эффективные алгоритмы и программы защиты информации.	умение находить и использовать информационный ресурс в процессе выполнения заданий по практике				
	Владеть: - навыками безопасного использования программно-аппаратных средств в системах защиты информации.	решение практических задач в конкретной предметной области				
ПК-12	Знать: - методы и средства противодействия атакам на ресурсы компьютерных систем.	знание и использование учебного материала в процессе выполнения заданий по практике				
	Уметь: - производить анализ и защиту от атак на ресурсы компьютерной системы.	умение находить и использовать информационный ресурс в процессе выполнения заданий по практике				
	Владеть: - методикой контроля целостности компьютерной системы.	решение практических задач в конкретной предметной области				
ПК-13	Знать: - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	знание и использование учебного материала в процессе выполнения заданий по практике				
	Уметь: - осуществлять рациональный выбор средств и методов защиты информации в телекоммуникационных системах.	умение находить и использовать информационный ресурс в процессе выполнения заданий по практике				
	Владеть: - методиками анализа результатов работы обнаружения вторжений.	решение практических задач в конкретной предметной области				

ПК-17	<p>Знать: - современные средства и методы мониторинга, технической диагностики средств защиты.</p>	<p>знание и использование учебного материала в процессе выполнения заданий по практике</p>				
	<p>Уметь: -выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности компьютерных систем.</p>	<p>умение находить и использовать информационный ресурс в процессе выполнения заданий по практике</p>				
	<p>Владеть: - средствами борьбы с атаками злоумышленников на технические и программно-аппаратные средства защиты компьютерных систем.</p>	<p>решение практических задач в конкретной предметной области</p>				
ПК-18	<p>Знать: - физическую организацию баз данных и принципы (основы) их защиты.</p>	<p>знание и использование учебного материала в процессе выполнения заданий по практике</p>				
	<p>Уметь: - разрабатывать эффективные процедуры и методы для защиты информации ограниченного доступа.</p>	<p>умение находить и использовать информационный ресурс в процессе выполнения заданий по практике</p>				
	<p>Владеть: - методиками анализа результатов работы обнаружения вторжений.</p>	<p>решение практических задач в конкретной предметной области</p>				
ПК-19	<p>Знать: - современные средства и методы мониторинга, технической диагностики средств защиты, оценки эффективности информационной безопасности компьютерных систем.</p>	<p>знание и использование учебного материала в процессе выполнения заданий по практике</p>				
	<p>Уметь: - выбирать необходимые инструментальные средства анализа</p>	<p>умение находить и использовать информационный ресурс в процессе</p>				

	защищенности компьютерных систем.	выполнения заданий по практике				
	Владеть: - средствами борьбы с атаками злоумышленников на ресурсы серверов баз данных.	решение практических задач в конкретной предметной области				
ПК-20	Знать: - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	знание и использование учебного материала в процессе выполнения заданий по практике				
	Уметь: - осуществлять рациональный выбор средств и методов защиты информации в компьютерных системах.	умение находить и использовать информационный ресурс в процессе выполнения заданий по практике				
	Владеть: - методами расчета и инструментального контроля показателей технической защищенности информации.	решение практических задач в конкретной предметной области				

7.2.7 Паспорт оценочных материалов

№п/п	Контролируемые разделы(темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Выполнение индивидуального задания по практике	ПК-2 ПК-3 ПК-5 ПК-6 ПК-8 ПК-12 ПК-13 ПК-17 ПК-18 ПК-19 ПК-20	Дневник практики, отчет по практике

7.3 Методические материалы, определяющие процедуры оценивания

язнаний,умений,навыкови(или)опытадеятельности

По итогам «Практики по получению профессиональных умений и опыта профессиональной деятельности» в качестве формы оценки знаний студентов используется: зачет с оценкой.

Зачет по практике проводится на кафедре или на базовом предприятии в последнюю неделю практики. На зачет студент предъявляет:

- отчет по практике, подписанный руководителем от предприятия и руководителем от кафедры;

- дневник практики с письменной характеристикой руководителя практики от предприятия с его подписью.

Студент отвечает на вопросы, связанные с выполнением индивидуального задания. Отметки выставляются по пятибалльной системе.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная:

1 Советов Б.Я., Яковлев С.А. Положение о производственной практике студентов Воронежского государственного технического университета.

– Воронеж. ВГТУ

–http://www.vorstu.ru/upravlenie/umu/doc/p_praktika.pdf.

2 Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб.пособие / А.А. Малюк. - М.: Горячая линия - Телеком, 2004. - 280 с. - ISBN 5-93517-197-X : 80-00. Допущено Мин. обр. РФ в качестве учеб.пособия для студентов вузов.

3 Бугров Ю.Г. Системные основы оценивания защиты информации [Электронный ресурс]: учеб.пособие / Ю. Г. Бугров, В. Б. Щербаков. - Электрон.текстовые, граф. дан. (1811Кб). - Воронеж: ВГТУ, 2005. – 1 электрон.опт. диск (CD-ROM). - 30-00.

Дополнительная:

1 Ермилов Е.В. Управление информационными рисками при атаках на АСУ ТП критически важных объектов [Электронный ресурс]: Учеб.пособие / Е. В. Ермилов [и др.]. - Электрон.текстовые, граф. дан. (544 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

2 Галатенко В.А. Стандарты информационной безопасности [Текст] / В. А. Галатенко; под ред. акад. РАН В.Б. Бетелина. М.: ИНТУ.РУ «Интернет – университет информации и технологий», 2006. – 204 с.

Галатенко, В. А.

Стандарты информационной безопасности / В.А. Галатенко. - 2-е изд. - Москва : Интернет-Университет Информационных Технологий, 2006. - 264 с. - (Основы информационных технологий). - ISBN 5-9556-0053-1.

URL: <http://biblioclub.ru/index.php?page=book&id=233065>

3 Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Руководящий документ [Текст]. – М.: Гостехкомиссия России, 2002. – 23 с.

4. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 21.07.2014) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа: <http://www.consultant.com>

Методические разработки:

1. Методические указания по производственной практике для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем» 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. О.В. Поздышева. - Электрон. текстовые, граф. дан. (243 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

<http://www.eios.vorstu.ru> (электронная информационно-обучающая система ВГТУ)

<http://e.lanbook.com/> (ЭБС Лань)

<http://znaniyum.com/> (ЭБС Знаниум)

<http://IPRbookshop.ru/> (ЭБС IPRbooks (Айбукс))

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

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

В подразделениях и лабораториях предприятий, являющихся базой для проведения производственной практики, должны быть предоставлены рабочие места для выполнения научно-исследовательских работ, в том числе с использованием компьютерной техники.

10 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

За время прохождения производственной практики студент должен выполнить следующие работы:

1. Разработка технического задания, патентно-информационный поиск.

2. Сбор фактического материала, необходимого для принятия правильного решения при выборе принципа работы, схемы и конструкции проектируемого средства защиты информации. Определение вопросов, требующих проработки научно – исследовательского характера. Разработка методики и плана этих исследований.

3. Сбор технического материала по вопросам организации и планирования процесса проектирования средств защиты информации на базе современных систем автоматизированного проектирования изделий, написание программы по теме исследования (при необходимости).