МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ П.Ю. Гусев
«31» августа 2021 г.

Рассмотрена и утверждена на ученом совете факультета от 31.08.2021 протокол №1

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

«Проектно-технологическая практика»

Специальность 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация специализация № 9 "Управление безопасностью телекоммуникационных систем и сетей"

Квалификация выпускника специалист по защите информации

Срок освоения образовательной программы 5 лет 6 мес.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ / О.В. Поздышева/

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

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2021

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 окружавшей среды, гражданской обороне.

2. ХАРАКТЕРИСТИКА ПРАКТИКИ

Вид практики – Производственная практика

Тип практика – Проектно-технологическая 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 практики устанавливается на основе типовых двусторонних договоров между предприятиями (организациями) и ВУЗом или ВУЗ.

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Практика «Проектно-технологическая практика» относится к части, формируемой участниками образовательных отношений блока Б.2 учебного плана.

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

Процесс прохождения практики «Проектно-технологическая практика» направлен на формирование следующих компетенций:

ПК-9.2 - способен участвовать в работах по проектированию и созданию систем защиты информации на объектах информатизации на основе изучения физических основ формирования технических каналов утечки информации;

ПК-9.5 - способен принимать участие в обеспечении функционирования и разработке средств и систем защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа (НСД).

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-9.2	**Знать:** - научные основы, цели, принципы, методы и технологии в сфере защиты информации; - существующие модели угроз информационной безопасности.
	Уметь: - оценивать риски, связанные с осуществлением угроз безопасности в отношении телекоммуникационной системы; - разрабатывать эффективные алгоритмы и программы защиты информации.
	Владеть: - навыками безопасного использования технических средств защиты информации; - навыками эффективного использования технических средств, применительно к заданным условиям эксплуатации.
ПК-9.5	**Знать:** - нормативные документы по защите информации; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.
	Уметь: - выбирать необходимые инструментальные средства анализа защищенности телекоммуникационных систем; - осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации.
	Владеть: - способами контроля доступа и защиты от несанкционированного доступа; - методами по разработке технологических процессов производства программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД.

5. ОБЪЕМ ПРАКТИКИ

Общая трудоемкость практики составляет 3 з.е., общая трудоемкость – 108 ч.

Форма промежуточной аттестации: зачет с оценкой.

6. СОДЕРЖАНИЕ ПРАКТИКИ

Распределение трудоемкости дисциплины по видам занятий

№ 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 предприятия (организации). Изучение нормативно-технической документации.	10
3	Практическая работа	Выполнение индивидуальных заданий. Сбор практического материала.	84
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	Зачет с оценкой	2
		Итого	108

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ

7.1 Подготовка отчета о прохождении практики

Аттестация по итогам практики проводится в виде зачета с оценкой на основе экспертной оценки деятельности обучающегося и защиты отчета. По завершении практики студенты в последний день практики представляют на выпускающую кафедру: дневник практики, включающий в себя отзывы руководителей практики от предприятия и ВУЗа о работе студента в период практики с оценкой уровня и оперативности выполнения им задания по

практике, отношения к выполнению программы практики 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 задание руководителя;
3 замечания руководителя;
4 содержание;
5 введение (цель практики, задачи практики);
6 практические результаты прохождения практики;
7 заключение;
8 список использованных источников и литературы;
9 приложения (при наличии).

7.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 6 семестре по четырехбальной системе:

«отлично»;
«хорошо»;
«удовлетворительно»;
«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл	Неудовл
ПК-9.2	**Знать:** - научные основы, цели, принципы, методы и технологии в сфере защиты информации; - существующие модели угроз информационной безопасности.	знание и использование учебного материала в процессе выполнения заданий по практике	Задание по практике выполнено в полном объеме. Студент демонстрирует ярко выраженную способность использовать знания, умения, навыки в процессе выполнения заданий	Студент демонстрирует значительное понимание материала. Студент демонстрирует способность использовать знания, умения, навыки в процессе выполнения заданий	Студент демонстрирует частичное понимание материала. Способность студента продемонстрировать знание, умение, навык выражена слабо	1. Задание по практике выполнено не полностью. 2. Студент демонстрирует непонимание заданий. 3. Студент не смог ответить на поставленные вопросы. 4. Не было попытки выполнить задание.
	Уметь: - оценивать риски, связанные с осуществлением угроз безопасности в отношении телекоммуникационной системы; - разрабатывать эффективные алгоритмы и программы защиты информации.	умение находить и использовать информационный ресурс в процессе полнения заданий по практике				
	Владеть: - навыками безопасного	решение практических задач в конкретной				

	использования технических средств защиты информации; - навыками эффективного использования технических средств, применительно к заданным условиям эксплуатации.	предметной области				
ПК-9.5	**Знать:** - нормативные документы по защите информации; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	знание и использование учебного материала в процессе выполнения заданий по практике				
	Уметь: - выбирать необходимые инструментальные средства анализа защищенности телекоммуникационных систем; - осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации.	умение находить и использовать информационный ресурс в процессе полнения заданий по практике				
	Владеть: - способами контроля доступа и защиты от несанкционированного доступа; - методами по разработке технологических процессов производства программных, программно-аппаратных (в том	решение практических задач в конкретной предметной области				

	числе криптографически х) и технических средств и систем защиты СССЭ от НСД.					

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

По итогам практики «Проектно-технологическая практика» 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;
- презентацию выполненной работы.

Студент отвечает на вопросы, связанные с тематикой практических занятий, индивидуального задания. Зачет может проходить в форме итоговой научно-практической студенческой конференции, на которую студенты представляют отчеты по индивидуальному заданию, при этом могут быть заданы любые вопросы по программе практики.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

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. Гончаров И.В. Построение сетей и систем передачи информации [Электронный ресурс]: Учеб. пособие / И. В. Гончаров. - Электрон. текстовые, граф. дан. (4,28 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

4. 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.
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:

Банк данных угроз безопасности информации. Электрон. дан. - Режим доступа: http://www.bdu.fstec.ru

Стандарт Common Vulnerabilities and Exposures. Электрон. дан. - Режим доступа: http://cve.mitre.org

База данных с информационными бюллетенями (Secunia Advisories),

содержащими сведения об обнаруженных угрозах и уязвимостях ПО Secunia Advisory and Vulnerability Database Электрон. дан. - Режим доступа: https://secuniaresearch.flexerasoftware.com/community/advisories

База уязвимостей VND (Vulnerability Notes Database Электрон. дан. - Режим доступа: https://www.kb.cert.org/vuls

База сценариев эксплуатации уязвимостей Exploit Database Электрон. дан. - Режим доступа: https://www.exploit-db.com

Агрегатор информации об уязвимостях CVEDetails. Электрон. дан. - Режим доступа: https://www.cvedetails.com

Information Security Информационная безопасность. Электрон. дан. - Режим доступа: http://www.itsec.ru

Securitylab.ru by Positive Technologies. Электрон. дан. - Режим доступа: https://www.securitylab.ru/

Anti-Malware.ru. Электрон. дан. - Режим доступа: https://www.anti-malware.ru/news

Iso27000.ru Искусство управления информационной безопасностью. Электрон. дан. - Режим доступа: http://www.iso27000.ru/

SecurityPolicy.ru Документы по информационной безопасности. Электрон. дан. - Режим доступа: http://securitypolicy.ru/

SearchInform – Информационная безопасность. Электрон. дан. - Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/

Информационная безопасность предприятия. Электрон. дан. - Режим доступа: Ekrost.ru

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

http://e.lanbook.com/ (ЭБС Лань)

http://znanium.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).
4. Подготовка отчёта и его защита.