МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Зам. директора по учебной работе
Пятигорского института (филиала) СКФУ
_____ М.В. Мартыненко

«___»_____ 20__г.

Рабочая программа по производственной практике
Преддипломная практика

Направление подготовки/специальность	10.03.01 Информационная безопасность
Направленность (профиль)/специализация	Безопасность компьютерных систем
Форма обучения	очная
Год начала подготовки	2022 г.
Реализуется в 8 семестре	

Разработано
Профессор кафедры СУиИТ
(должность разработчика)
Першин И.М.
Ф.И.О.

Пятигорск, 2022 г.

Введение

Методические указания по организации преддипломной практики разработаны в соответствии с требованиями ФГОС ВО с учетом рекомендаций ОП по направлению и профилю подготовки 10.03.01 «Информационная безопасность», «Положением о порядке проведения практики студентов» и учебным планом направления 10.03.01 «Информационная безопасность».

Методические указания по организации учебной практики предназначены для студентов всех форм обучения направления подготовки бакалавров 10.03.01 «Информационная безопасность» и содержат материалы по организации, проведению и контролю прохождения практики, примерному распределению времени в период практики; указывают обязанности студентов, ставят задачи практики, содержат индивидуальные и теоретические задания и требования к оформлению результатов учебной исследовательской практики.

Учебная практика студентов является составной частью основной образовательной программы высшего профессионального образования подготовкивысококвалифицированных специалистов, представляет собой вид учебных занятий, непосредственно ориентированных на практическую подготовку обучающихся.

1. Цели практики

Целями преддипломной практики по направлению подготовки 10.03.01 Информационная безопасность являются:

1) закрепление, расширение, углубление и систематизация знаний, полученных приизучении специальных дисциплин;
2) приобретение практических навыков и компетенций в сфере профессиональнойдеятельности;
3) подбор необходимого материала для выполнения дипломного проектирования.

2. Задачи практики:

Задачами преддипломной практики являются:

1) Изучить:
- современные аппаратные и программные средства вычислительной техники;
- принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны;
- конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации;
- перспективные каналы утечки информации, способы их выявления и методы оценки опасности;
- основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;

- методы и средства инженерно-технической защиты информации;
- принципы и методы противодействия несанкционированному информационномувоздействию на вычислительные системы и системы передачи информации;
- принципы построения современных криптографических систем, стандарты в областикриптографической защиты информации;
- основные правовые положения в области информационной безопасности и защитыинформации.

2) Освоить:
- методы организации и управления деятельности служб защиты информации напредприятии;
- технологии проектирования, построения и эксплуатации комплексных систем защитыинформации;
- методы научных исследований уязвимости и защищенности информационныхпроцессов;
- методики проверки защищенности объектов информатизации на соответствиетребованиям нормативных документов.

3) Подобрать, изучить и обобщить научно-техническую литературу, нормативно- методические материалы по инженерно-технической защите информации. Научиться внедрять комплексные системы и отдельные специальные технические и программно- математические средства защиты информации на объектах информатизации, в том числе сравнительного анализа типовых криптосхем. Разработать предложения по совершенствованию и повышению эффективности применяемых мер на основе анализа результатов контрольных проверок, изучения и обобщения опыта эксплуатации объекта информатизации. Участвовать в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности. Знать вопросы нормирования, организации и оплаты труда, вопросы обеспечения безопасностижизнедеятельности на предприятии.

3. Место практики в структуре образовательной программы

Преддипломная практика относится к блоку 2 «Практики», ее освоение происходит в8-м семестре. Практика базируется на следующих дисциплинах: «Основы информационной безопасности», «Методы проектирования систем технической охраны объектов информатизации», «Эксплуатационная практика».

Для освоения программы практики, обучающиеся должны владеть следующими знаниями и компетенциями:
- способностью к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональнойдеятельности;
- использованием на практике умений и навыков в организации исследовательских и проектных работ, в управлении коллективом.

Результаты прохождения практики должны быть использованы в дальнейшем в подготовке выпускных квалификационных работ.

4. Место и время проведения практики

Преддипломная практика проводится на 4 курсе в 8 семестре в течение 6 недель на основании учебного плана для данного направления подготовки.

Преддипломная практика может проводиться в структурных подразделениях организаций (предприятий и фирм) различных форм собственности на основе прямых договоров, заключаемых между организацией и университетом. При наличии вакантных должностей студенты могут зачисляться на них, если работа соответствует требованиям программы практики.

Рабочие места для студентов могут выделяться в структурных подразделениях, связанных с исследованиями, проектированием, организацией и эксплуатацией информационных систем и систем защиты информации. К таким подразделениям относятся:

1) научно-исследовательские отделы;
2) конструкторские отделы;
3) технологические отделы;
4) отделы испытаний;
5) отделы и лаборатории, занимающиеся автоматизацией проектирования и управления производством;
6) службы АСУ;
7) службы режима работы предприятия.

В этих подразделениях студенты-практиканты могут выполнять функции разработчика, исследователя, программиста и т.п. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

5. Перечень планируемых результатов по практике, соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты, характеризующие этапы формирования компетенций, индикаторов
ПК-1	ИД-1 ПК-1 Понимает порядок обслуживания криптографических средств защиты информации. ИД-2 ПК-1. Имеет навыки обслуживать технические средства защиты информации. ИД-3 ПК-1 Владеет навыками эксплуатации программно-аппаратных и технических средств защиты информации.	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-2	ИД-1 ПК-2 Знает методы и средства разработки программного обеспечения. ИД-2 ПК-2 Способен оценивать средства разработки программ. ИД-3 ПК-2 Обладает методами программирования на языках [illegible] для решения профессиональных задач.	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК-3	ИД-1 ПК-3 Понимает угрозы	Способность администрировать

	безопасности, режимы противодействия. ИД-2 ПК-3 Способен определять состав и порядок администрирования подсистемы информационной безопасности. ИД-3 ПК-3 Обладает навыками мониторинга функционирования подсистемы ИБ.	подсистемы информационной безопасности объекта защиты
ПК-4	ИД-1 ПК-4 Имеет знания виды комплексного подхода в организации политики информационной безопасности. ИД-2 ПК-4 Умеет формулировать, настраивать политики безопасности. ИД-3 ПК-4 Владеет навыками формулирования и контролирования соблюдения требований политики безопасности.	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-5	ИД-1 ПК-5 Знает нормативную документацию по аттестации объектов информатизации. ИД-2 ПК-5 Способен выполнять требования безопасности хранения и обработки информации. ИД-3 ПК-5 Обладает навыками аттестации объектов информации по средствам требований информатизации.	Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-6	ИД-1 ПК-6. Знает методы и принципы проведения аудита информационной безопасности. ИД-2 ПК-6 Способен организовывать и проводить аудит работоспособности и эффективности применяемых средств защиты информации. ИД-3 ПК-6 Владеет навыками оценивания оптимальности выбора программно-аппаратных средств защиты информации	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-7	ИД-1 ПК-7 Знает требования по защите информации, включая использование математического аппарата для решения прикладных задач. ИД-2 ПК-7 Умеет составлять планы этапов проведения научно-исследовательских и опытно-конструкторских работ. ИД-3 ПК-7 Владеет навыками	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

	разработки и анализа структурных и функциональных схем защищенных компьютерных систем в сфере профессиональной деятельности.	
ПК-8	ИД-1 ПК-8 Понимает действующие нормативные и методические документы. ИД-2 ПК-8 Способен анализировать, систематизировать, оформлять техническую документацию. ИД-3 ПК-8 Владеет навыками грамотного составления технической документации	Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
ПК-9	ИД-1 ПК-9 Знает методы поиска научно-технической информации. ИД-2 ПК-9 Способен выбирать необходимую информацию в области информационной безопасности; составлять обзор по вопросам обеспечения информационной безопасности. ИД-3 ПК-9 Владеет навыками изучения научно-технической литературы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
ПК-10	ИД-1 ПК-10 Понимает международные и отечественные стандарты соответствия объектов информационной безопасности. ИД-2 ПК-10 способен применять стандарты при анализе на соответствие объектов информационной безопасности. ИД-3 ПК-10 Владеет методами проведения анализа объектов информационной безопасности.	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
ПК-11	ИД-1 ПК-11 Знает методы обработки и анализа результатов проведения экспериментов. ИД-2 ПК-11 Умеет выбирать необходимые методы для обработки и анализа результатов проведения экспериментов. ИД-3 ПК-11 Владеет навыками обработки и анализа	Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

	результатов проведения экспериментов по изучению и тестированию системы обеспечения информационной безопасности или ее отдельных элементов.	
ПК-12	ИД-1 ПК-12 Понимать принципы функционирования системы защиты информации. ИД-2 ПК-12 способен проводить исследования описывая каждый этап эксперимента и обосновывать полученный результат. ИД-3 ПК-12 Владеет методами анализа процедуры исследования и результата согласно заданным критериям.	Способность принимать участие в проведении экспериментальных исследований системы защиты информации

6. Структура и содержание учебной практики

Общая трудоемкость учебной практики составляет 9 зачетных единиц - 243 часов.

Разделы (этапы) практики	Реализуемые компетенции / индикаторы	Виды учебной работы на практике, включая самостоятельную работу студентов	Трудоемкость (час.)	Формы текущего контроля
Подготовительный этап (инструктаж технике безопасности)	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12	ознакомительные лекции	18	Устный отчет
Экспериментальный этап:	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12	инструктаж по технике безопасности	34	Письменный отчет
1.Закрепление теоретических и Практических навыков работы с программно-аппаратными средствами защиты, а также техническими средствами охраны в лабораториях кафедры СУИИТ;	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12	мероприятия по сбору, обработке и систематизации фактического и литературного материала	36	Проверка отчета
2. Установка, настройка, эксплуатация и поддержание в работоспособном	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12	Мероприятие по наблюдению, измерению работ	52	Проверка отчета

состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;				
3.Проработка индивидуального теоретического задания по вариантам;	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12	мероприятия по сбору, обработке и систематизации фактического и литературного материала	36	Проверка отчета
4. Решение индивидуального практического задания по вариантам;	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12	Мероприятие по наблюдению, измерению работ	32	Проверка отчета
5. Подготовка и оформление отчета.	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12	мероприятия по сбору, обработке и систематизации фактического и литературного материала	32	Проверка отчета
Заключительный этап (защита отчета)	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12		3	Защита отчета по практике
Итого			243	-

6. Методические рекомендации для студентов по прохождению практики

6.1. Использование материала учебно-методического комплекса практики

На первом этапе необходимо ознакомиться со структурой практики, обязательными видами работ и формами отчетности.

Для успешного выполнения заданий по ознакомительной практике, студенту необходимо выполнить задания по практике

В процессе прохождения преддипломной практики используются интерактивные методы и технологии, которые формируют общекультурные компетенции у студентов за счет:

– лекций и консультаций с применением мультимедийных технологий;

– самостоятельных работ с использованием ПК и современного лабораторного оборудования.

6.2. Фонд оценочных средств по практике

Фонд оценочных средств (ФОС) по преддипломной практике базируется на перечне осваиваемых компетенций с указанием этапов их формирования в процессе

прохождения практики. ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций;

- типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений и уровня овладения формируемыми компетенциями в процессе прохождения практики.

ФОС является приложением к данной программе практики.

8. Учебно-методическое и информационное обеспечение практики

8.1. Рекомендуемая литература

8.1.1. Основная литература

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2018.— 266 с.— Режим доступа: http://www.iprbookshop.ru/52209.— ЭБС «IPRbooks», по паролю

2. Методы проектирования систем технической охраны объектов : лабораторный практикум / сост. И.В. Калиберда ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2019. - 129 с. - Библиогр. в конце глав

8.1.2. Дополнительная литература:

3. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2017.— 154 с.— Режим доступа: http://www.iprbookshop.ru/52160.— ЭБС «IPRbooks», по паролю.

4. Методы проектирования систем технической охраны объектов : учеб. пособие / П.П. Мулкиджанян, Ю.Г. Айвазов, В.В. Родишевский и др. ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2017. - 163 с. - Прил.: с. 83-159. - Библиогр.: с. 82

8.1.3. Методическая литература:

1. Методические указания по организации и проведению учебной практики –

«Ознакомительная практика» для студентов направления 10.03.01 «Информационная безопасность».

2. Инструкции по технике безопасности и охране труда при работе в лабораториях кафедры

Методические рекомендации для оформления рефератов, отчетов по практике, курсовыхработ/проектов, выпускных квалификационных работ Пятигорск: 2020 г. – 20 с.

8.1.4. Интернет-ресурсы:

1. http://elibrary.ru - Научная электронная библиотека eLIBRARY.RU
2. http://www.biblioclub.ru -Университетская библиотека online

8.2 Программное обеспечение:

1С: Предприятие 8 - комплект для обучения в высших и средних учебных заведениях (регистр. № 0334708), AutoCAD 2015 (бесплатный для вузов), Embarcadero rad studio - Г/к 445/01 от 30 июля 2010 г., IBM Rational Rose modeler (бесплатно по программе

IBM Academic Initiative), Mathcad Education - University Edition (50 pack) -договор № 24-эа/15 от 19 августа 2015г., Microsoft Office - №61541869, Cisco Packet Tracer - договор № 23-с от 27 июня 2012 г., Microsoft Windows 7 Профессиональная - №61541869, Visual Studio IDE – AzureDev ID: a6c2b0d7-162e-479f-8a58-384701f33665, Microsoft Visual Basic – AzureDev ID: a6c2b0d7-162e-479f-8a58-384701f33665, Microsoft SQL Server – AzureDev ID: a6c2b0d7- 162e-479f-8a58-384701f33665, PascalABC.NET (бесплатный), Oracle VM VirtualBox (бесплатный).

8.3 Материально-техническое обеспечение практики

Определяется структурой места прохождения практики, если практика проходит на кафедре ВУЗа используется следующее материально-техническое обеспечение: специализированная учебная мебель и технические средства обучения, служащие для представления учебной информации: компьютеры (5 шт) с подключением к сети "Интернет" и доступом в электронную информационно-образовательную среду, книжные шкафы для учебной литературы и учебно-методических материалов

8.4 Особенности освоения практики лицами с ограниченными возможностями здоровья: Специальных условий освоения практики не требуется.