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
Технологическая практика

Направление подготовки — 10.03.01 Информационная безопасность
Направленность (профиль) — Безопасность компьютерных систем
Форма обучения — очная
Год начала подготовки — 2023 г.
Реализуется в 6 семестре

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

Пятигорск, 2023

1. Цели практики студентов

Целью производственной технологической практики являются закрепление и углубление знаний, полученных студентами в процессе теоретического обучения, приобретение необходимых умений, навыков, компетенций и опыта практической работы по изучаемому направлению.

2. Задачи практики

Задачами технологической практики является:

– получения практических навыков самостоятельной и коллективной работы при решении поставленных задач;

– углубленное изучение и приобретение практических навыков в работе с системами криптографической защиты в рамках конкретного предприятия;

– изучение технологий внедрения, настройки и применения межсетевых экранов, траффик-инспекторов и других технологий защиты информации в компьютерных сетях организаций;

– изучение возможностей VPN-технологий для защиты информации на предприятии;

– приобретение и закрепление практических навыков работы с программно-аппаратными средствами защиты информации на предприятиях.

3. Место практики в структуре ООП бакалавриата

Технологическая практика непосредственно ориентирована на профессионально- практическую подготовку обучающихся. Технологическая практика базируется на освоении таких дисциплин как «Методы и средства криптографической защиты информации», «Техническая защита информации», «Защита информации от утечки по техническим каналам».

Технологическая практика является одним из основных видов профильной подготовки студентов и представляет собой комплексные практические занятия, дополненные другими видами учебного процесса, в ходе которых происходит ознакомление с устройствами и программным обеспечением в области защиты информации и дальнейшее формирование профессиональных знаний.

Для успешного прохождения учебной технологической практики студент должен обладать «входными» знаниями, умениями и готовностями, приобретенными в результате освоения предшествующих частей ОП, а именно:

знать:

– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– технологии обнаружения компьютерных атак и их возможности;

– средства реализации атак.

– механизмы типовых атак, основанных на уязвимостях сетевых протоколов.

– атаки на сетевые службы.

– атаки с использованием промежуточных узлов и территорий.

– основные уязвимости и типовые атаки на современные компьютерные системы;

– возможности и особенности использования

специализированных программно- аппаратных средств при проведении аудита информационной безопасности;
- методы защиты компьютерных сетей;
- классификацию и общую характеристику сетевых программно-аппаратных средств защиты информации;
- основные принципы администрирования защищенных компьютерных систем;
- особенности реализации методов защиты информации современными программно- аппаратными средствами.

уметь:

- выполнять функции администратора безопасности защищенных компьютерных систем;
- выполнять настройку защитных механизмов сетевых программно-аппаратных средств;
- настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации;
- применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей;
- организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов;
- применять средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети.
- Реализовывать цели и принципы зондирования узлов сети.
- Использовать коммерческие и свободно распространяемые средства аудита безопасности компьютерных сетей.
- Использовать особенности средств активного аудита.
- применять средства анализа защищенности серверов приложений.

владеть:

- средствами администрирования сетевых программно-аппаратных комплексов защиты информации;
- средствами администрирования систем обнаружения компьютерных атак;
- средствами и системами аудита информационной безопасности; методикой проведения аудита информационной безопасности;
- средствами администрирования систем организации виртуальных частных сетей.
- Навыками определения структуры информационно-телекоммуникационных сетей.
- Навыками применения программных средств анализа топологии вычислительной сети, определения маршрутов прохождения сетевых пакетов, обнаружения объектов сети, построения схемы сети.
- Навыками выявления телекоммуникационного оборудования, выявления и построения схемы информационных потоков защищаемой информации в компьютерной сети.

4. Место и время проведения практики

Производственная технологическая практика проводится на 3 курсе в 6 семестре продолжительностью две недели. Производственная технологическая практика проводится на предприятиях профиля данной специальности, оснащенных современным технологическим оборудованием и компьютерной техникой.

5. Компетенции обучающегося, формируемые при прохождении практики

5.1 Наименование компетенции

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты, характеризующие этапы формирования компетенций, индикаторов

и		
ОПК-7	ИД-1 ОПК-7 Знает языки программирования и системы разработки программных средств для решения профессиональных задач. ИД-2 ОПК-7 Способен выбирать необходимые языки программирования и системы разработки программных средств для решения профессиональных задач. ИД-3 ОПК-7 Обладает навыками применения языков программирования и систем разработки программных средств для решения профессиональных задач.	Способен использовать языки программирования и технологии разработки программах средств для решения задач профессиональной деятельности
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-3	ИД-1 ПК-3 Понимает угрозы 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.	Способность администрировать подсистемы 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 информатизации	Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

5. Структура и содержание учебной практики

Общая трудоемкость учебной практики составляет 3 зачетных единиц – 81 часов.

Разделы (этапы) практики	Реализуемые компетенции /		Виды учебной работы на практике, включая	Трудоемкость (час.)	Формы текущего контроля

	индикаторы	самостоятельную работу студентов		
Подготовительный этап (инструктаж технике безопасности)	ОПК-7, ПК-1, ПК-3, ПК-5	ознакомительные лекции	12	Устный опрос
Экспериментальный этап:	ОПК-7, ПК-1, ПК-3, ПК-5	инструктаж по технике безопасности	12	Проверка письменного отчета о работе со средствами защиты
1.Закрепление теоретических и Практических навыков работы с программно-аппаратными средствами защиты, а также техническими средствами охраны в лабораториях кафедры СУИИТ;	ОПК-7, ПК-1, ПК-3, ПК-5	мероприятия по сбору, обработке и систематизации фактического и литературного материала	12	Проверка отчета
2. Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;	ОПК-7, ПК-1, ПК-3, ПК-5	Мероприятие по наблюдению, измерению работ	12	Проверка отчета
3.Проработка индивидуального теоретического задания по вариантам;	ОПК-7, ПК-1, ПК-3, ПК-5	мероприятия по сбору, обработке и систематизации фактического и литературного материала	10	Проверка отчета
4. Решение индивидуального практического задания по вариантам;	ОПК-7, ПК-1, ПК-3, ПК-5	Мероприятие по наблюдению, измерению работ	10	Проверка отчета
5. Подготовка и оформление отчета	ОПК-7, ПК-1, ПК-3, ПК-5	мероприятия по сбору, обработке и систематизации фактического и	10	Проверка отчета

		литературного материала		
Заключительный этап (защита отчета)	ОПК-7, ПК-1, ПК-3, ПК-5		3	-
Итого			81	-

6. Методические рекомендации для студентов по прохождению практики

7.1. 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 учебной ознакомительной 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

7. Фонд оценочных средств по практике

Фонд оценочных средств (ФОС) по технологической 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.

9. Учебно-методическое и информационное обеспечение практики

9.1. Рекомендуемая литература

9.1.1. Основная литература:

1. Леонова О.В. Основы научных исследований [Электронный ресурс]: учебное пособие/ Леонова О.В.— Электрон. текстовые данные.— М.: Московская государственная академия водного транспорта, 2017.— 70 с.— Режим доступа: http://www.iprbookshop.ru/46493.— ЭБС «IPRbooks», по паролю.

2. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон.текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2018.— 424 с.

3. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2018. - 369 с.

4. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2018. - 572 с.

5. Системы защиты информации в ведущих зарубежных странах : учебное

пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2018. - 224 с.

9.1.2. Дополнительная литература:

1. Лонцева И.А. Основы научных исследований [Электронный ресурс]: учебное пособие/ Лонцева И.А., Лазарев В.И.— Электрон. текстовые данные.— Благовещенск: Дальневосточный государственный аграрный университет, 2017.— 185 с. — Режим доступа: http://www.iprbookshop.ru/55906.— ЭБС «IPRbooks», по паролю.
2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. : [учебник] / В.Г. Олифер, Н.А. Олифер. - 4-е изд. - СПб. : Питер, 2017. - 944 с.
3. Таненбаум, Э. Компьютерные сети : [учеб. пособие] / Э. Таненбаум ; пер. с англ. В. Шрага. - 4-е изд. - СПб. : Питер, 2017. - 992 с. .
4. Сети и телекоммуникации : учеб.пособие / Б.В. Соболь, А.А. Манин, М.С. Герасименко. - Ростов н/Д : Феникс, 2018. - 191 с. .
5. Галицкий, А. В. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. - М. : ДМК Пресс, 2017. - 616 с.

9.1.3. Методическая литература:

1. Методические указания по организации и проведению учебной практики –

«Технологическая 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, курсовых работ/проектов, выпускных квалификационных работ Пятигорск: 2020г. – 20 с.

9.1.4. Интернет-ресурсы:

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

9.2 Программное обеспечение: Специальное программное не требуется

9.3 Материально-техническое обеспечение практики (в соответствии с образовательным стандартом)

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 переносной проектор Acer PO100 экран LUMA 1300, ноутбук (1 шт) Asus K50I T44002.2/3072/GT320M/250/5400/DVD-RW, наборы демонстрационного оборудования и учебно-наглядных пособий

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