ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» (СПбГУТ)

СМОЛЕНСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ (ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА».

КТ СМОЛЕНСК

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 009533997B26BB162CCCB9A17C8FD30591
Владелец: Иванешко Ирина Васильевна
Действителен: с 22.05.2023 до 14.08.2024

Утверждаю
Зам. директора по учебной работе
_____ И.В. Иванешко
«31» 08 2023г.

РАБОЧАЯ ПРОГРАММА

производственной практики ПП.02.01

в составе

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических, средств защиты

по специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

г. Смоленск

2023

Рассмотрено на заседании
методической комиссии компьютерных
сетей и администрирование
Председатель _____ О.С. Скряго
Протокол № 1
«31» 08 2023

Составитель: Драницина М.Д.- заведующий практикой СКТ(ф) СПбГУТ

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Министерства образования и науки РФ от 09.12.2016г. №1551, а также на основании примерной основной образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, разработанной ФУМО в системе СПО по УГС 10.00.00 «Информационная безопасность».

Согласовано: Руководитель направления Управления безопасности Смоленского филиала ПАО «Ростелеком» _____ Петров В.А.

М.П.

2

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ

Производственная практика ПМ.02

1.1. Область применения программы

Программа производственной практики по ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты является частью образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в части приобретения практического опыта в процессе освоения основного вида профессиональной деятельности (ВД): Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи и соответствующих профессиональных (ПК) и общих (ОК) компетенций:

Код	**Наименование видов деятельности и профессиональных компетенций**
ВД 2.	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты
ПК 2.1	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 09. Использовать информационные технологии в профессиональной деятельности.
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

1.2. Цели и задачи практики, требования к результатам освоения

Производственная практика в виде практической подготовки направлена на формирование у обучающихся умений, приобретение первоначального практического опыта и реализуется в рамках модулей ПООП (примерные основные образовательные программы) СПО по основным видам профессиональной деятельности для последующего освоения ими общих и профессиональных компетенций по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем: квалификация - **техник по защите информации**

Производственная практика базируется на междисциплинарных курсах профессионального модуля:

- МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты;
- МДК.02.02. Криптографическая защита информации.
- УП.02.01.

С целью освоения указанного вида профессиональной деятельности и соответствующих профессиональных компетенций в результате прохождения практической подготовки обучающийся должен:

Иметь практический опыт в	ПО1 установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей; ПО2 поддержании бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях; ПО3 защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.
уметь	У1 выявлять и оценивать угрозы безопасности информации в ИТКС; У2 настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; У3 проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации; У4 проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации; У5 проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; У6 проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; У7 проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации.
знать	З1возможные угрозы безопасности информации в ИТКС; З2 способы защиты информации от несанкционированного доступа (далее - НСД) и специальных воздействий на нее;

	З3 типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях; З4 криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях; З5 порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации; З6 организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации; З7 порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации.

Вариативная часть

С целью удовлетворения запросов рынка труда и обеспечения конкурентоспособности выпускника студент должен:

иметь практический опыт	ПО4 определения необходимых средств криптографической защиты информации;
уметь	У8 определять рациональные методы и средства защиты на объектах и оценивать их эффективность; У9 пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
знать	З8 типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; З9 основные протоколы идентификации и аутентификации в телекоммуникационных системах; З10 особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;

1.3. Количество часов на освоение программы производственной практики: 180 часов.

Для выполнения программы практики обучающийся должен иметь практический опыт, полученный в результате освоения междисциплинарных курсов и учебных практик профессионального модуля ПМ.02 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических, средств защиты».

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРАКТИКИ

2.1. Результатом освоения программы учебной и производственной практики профессионального модуля ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических, средств защиты является овладение профессиональными (ПК) и общими (ОК) компетенциями.

3. СТРУКТУРА СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ ПО ПМ.02. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ, В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИХ, СРЕДСТВ ЗАЩИТЫ ПО СПЕЦИАЛЬНОСТИ: 10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Код профессиональных компетенций	**Наименования профессионального модуля, МДК**	**Количество часов на производственную практику по ПМ.03, по соответствующему МДК**	**Виды работ**
ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических, средств защиты			
ПК 2.1 ПК 2.2 ПК 2.3	МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты.	18	Участие в организации работ по защите персональных компьютеров на предприятии
		18	Участие в организации работ по защите локальных сетей на предприятии
		18	Участие в организации работ по защите работ в глобальной сети интернет на предприятии
		18	Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети
		18	Администрирование систем безопасности проводной защищенной локальной сети
ПК 2.1 ПК 2.2 ПК 2.3	МДК.02.02. Криптографическая защита информации.	12	Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети
		12	Администрирование систем безопасности беспроводной защищенной локальной сети
		12	Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей

		6	Выбор программных средств шифрования в соответствии с решаемой задачей
		12	Подключение, установка драйверов, настройка программных средств абонентского шифрования
		6	Администрирование внедренных средств
		12	Настройка средств электронной подписи
		6	Администрирование средств электронной подписи
		6	Администрирование средств PKI
		6	Сдача технического отчета, получение оценки КДЗ
ВСЕГО часов		**180**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Производственная практика по профессиональному модулю 02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических, средств защиты по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем проходит на базе предприятий, учреждений и организаций различных организационно-правовых форм и форм собственности на основе договоров, заключаемых между предприятием и колледжем, отвечающим следующим требованиям:

- наличие сфер деятельности, предусмотренных программой производственной практики;
- обеспечение квалифицированными кадрами для руководства производственной практикой.

Колледж имеет договоры о практической подготовке обучающихся специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем с предприятиями:

ПАО «Ростелеком»;
ОО «Ман-сеть»;
ООО Т2 Мобайл;
АО «НИИ СТТ» ;
ОГАУЗ «СОМИАЦ»;
ООО «Ситиком».

Для прохождения производственной практики на предприятиях организованы технически оснащенные рабочие места практиканта:
Локальная сеть с выходом в Интернет PROXY-SERVER.
Компьютер персональный.
Специализированное программное обеспечение систем приема; передачи и обработки сигналов.
Комплекс «Защита объекта от утечки информации по техническим каналам».
Сервер Dell PowerEdge .
Комплект нормативных документов.

4.2. Информационное обеспечение обучения

1. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182491 (дата обращения: 22.09.2022). — Режим доступа: для авториз. пользователей.
2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87995 (дата обращения: 22.09.2022). — Режим доступа: для авторизир. пользователей
3. Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ (МИИТ), 2019. — 144 с. — ISBN 978-5-7876-0326-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188703 (дата обращения: 22.09.2022). — Режим доступа: для авториз. пользователей

4.3. Общие требования к организации практики

К прохождению производственной практики допускаются обучающиеся, не имеющие академической задолженности по междисциплинарным курсам и учебным практикам в рамках освоения профессионального модуля ПМ.02. Защита информации в информационно-

телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических, средств защиты по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Организация производственной практики осуществляется в сроки, установленные рабочим учебным планом, после изучения всего раздела междисциплинарного курса или чередуясь с темами теоретического обучения.

Максимальный объем производственной практики составляет 36 академических часов в неделю.

База практики должна соответствовать профилю специальности обучающегося.

На предприятии за студентом закрепляется руководитель, который проводит с ним инструктаж по технике безопасности, охране труда, знакомит обучающегося со структурой предприятия, помогает освоить темы производственной практики и осуществляет контроль ее прохождения. В колледже подготовкой обучающегося к производственной практике, консультацией по вопросам прохождения практики занимается заведующий практикой.

Во время прохождения практики обучающийся ведет дневник практики, в котором руководитель от предприятия делает отметки и выставляет оценки. В конце практики студент оформляет отчет по производственной практике, согласно требованиям по составлению технического отчета. Руководитель практики от предприятия дает отзыв-характеристику о сформировавшихся у практиканта общих и профессиональных компетенциях, что учитывается в дальнейшем при получении итоговой оценки по практике.

Аттестация по итогам производственной практики (по профилю специальности) проводится с учетом результатов ее прохождения, подтверждаемых документами соответствующих организаций (баз практик). Студент должен представить в колледж для получения оценки по практике: технический отчет с выполненным заданием, заполненный дневник, аттестационный лист, который выдается студентам в колледже.

4.4. Кадровое обеспечение практики

Требования к квалификации руководителей, осуществляющих руководство практикой от предприятий: дипломированные специалисты, имеющие высшее образование. Общее руководство практикой на предприятии возлагается на руководителя предприятия, организации, заместителя или одного из ведущих специалистов. Руководителем практики назначается должностное лицо из числа инженерно-технического состава.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРАКТИКИ ВПД «ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ, В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИХ, СРЕДСТВ ЗАЩИТЫ»

Одной из форм контроля результатов производственной практики является дневник практики, который ведется обучающимся в процессе прохождения практики.

По результатам прохождения производственной практики обучающийся составляет технический отчет, который утверждается организацией, на базе которой проходила практика. В качестве приложения к дневнику практики обучающийся оформляет материалы по индивидуальному заданию на практику, а так же графические, аудио-, фото-, видео-, материалы, подтверждающие практический опыт, полученный на практике.

Результаты (освоенные ПК)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить техническое	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

	обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	
ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные ОК)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ОК 09. Использовать информационные технологии в профессиональной деятельности	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ОК10 Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания