

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Липецкий филиал Финуниверситета

СОГЛАСОВАНО

ПАО «Ростелеком»

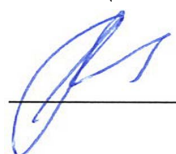
Директор Липецкого филиала
ПАО «Ростелеком»


_____ К.В. Власов

«29» августа 2024 г.

УТВЕРЖДАЮ

Заместитель директора
по учебно-методической работе
Липецкого филиала Финуниверситета


_____ О.Н. Левчegov

«29» августа 2024 г.

РАБОЧАЯ ПРОГРАММА
производственной практики (по профилю специальности) для ПМ.03. Защита
информации в информационно-
телекоммуникационных системах и сетях с использованием технических
средств защиты

по специальности 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

Липецк - 2024

Рабочая программа производственной практики (по профилю специальности) разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Разработчики:

Якушов Юрий Алексеевич, старший преподаватель кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Рабочая программа производственной практики (по профилю специальности) рассмотрена и рекомендована к утверждению на заседании кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Протокол от 27.08.2024 г. №1

Заведующий кафедрой

Учет и информационные технологии в бизнесе _____ Н.С. Морозова

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	6
2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)	8
3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)	13
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)	15

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Рабочая программа производственной практики для профессионального модуля **ПМ.03. «Защита информации в информационно- телекоммуникационных системах и сетях с использованием технических средств защиты»** является частью основной образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (квалификация – техник по защите информации) в части освоения основных видов деятельности:

– Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты;

Область профессиональной деятельности выпускников: Область профессиональной деятельности выпускников: 06 Связь, информационные и коммуникационные технологии. 12 Обеспечение безопасности.

1.1. Цель и планируемые результаты освоения программы производственной практики

Производственная практика (по профилю специальности) направлена на формирование у обучающихся общих и профессиональных компетенций, освоение современных производственных процессов, адаптация обучающихся к конкретным условиям деятельности организаций различных организационно-правовых форм, приобретение практического опыта в рамках профессиональных модулей ППССЗ СПО по каждому из основных видов профессиональной деятельности предусмотренных ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (квалификация – техник по защите информации).

Результатом освоения программы производственной практики (по профилю специальности) для профессионального модуля ПМ.03. «Защита информации в информационно - телекоммуникационных системах и сетях с использованием технических средств защиты» является сформированность у обучающихся практических профессиональных умений, приобретение первоначального практического опыта, необходимых для последующего освоения ими общих (ОК) и профессиональных (ПК) компетенций по 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

1.1.1. Перечень общих компетенций

Код	Наименование компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно

	действовать в чрезвычайных ситуациях
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

Код	Наименование компетенции
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях.
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях
ПК 3.3.	Осуществлять защиту информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно – телекоммуникационных систем и сетей

В результате прохождения производственной практики (по профилю специальности), реализуемой в рамках модуля ПМ.03. «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» ППССЗ СПО по каждому из основных видов деятельности (ОВД), предусмотренных ФГОС СПО, обучающийся должен приобрести практический опыт работы:

Основной вид деятельности	Умения и практический опыт в
Защита информации в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты	Уметь:
	проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
	проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
	проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
	проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
	использовать средства физической защиты линий связи ИТКС;
	применять нормативные правовые акты и нормативные методические документы в области защиты информации;
	Иметь практический опыт в:
	установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;
	защите информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
	проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

1.2 Количество часов на освоение рабочей программы производственной практики (по профилю специальности)

Всего 468 часов, в том числе:

В рамках освоения ПМ.03 –108 часов.

2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

2.1. Структура программы производственной практики (по профилю специальности)

Коды профессиональных компетенций	Наименования профессиональных модулей и МДК	Объем часов
ПК 3.1 – ПК 3.4	ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	108
Всего часов		108

2.2. Содержание производственной практики (по профилю специальности)

Код и наименование профессиональных модулей, МДК и тем производственной практики (по профилю специальности)	Виды работ		Объем часов
ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	Содержание производственной практики (по профилю специальности)		
	1	Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Получение заданий по тематике	108
	2	Определение исходных данных по защищаемому объекту и плана работ по созданию системы защиты речевой информации (СЗРИ)	
	3	Выявление технических каналов утечки (ТКУ) речевой информации с использованием современных средств контроля и контрольно-измерительной аппаратуры	
	4	Подготовка предложений в проект технического задания на создание СЗРИ, в том числе специального защищенного (экранированного) помещения (СЗП)	
	5	Разработка рекомендаций по совершенствованию мер защиты речевой информации и предложения по корректировке СЗРИ и СЗП	
	6	Монтаж средств защиты информации и их настройка, инструментальная оценка эффективности защиты речевой информации и электромагнитного экранирования СЗП	
	7	Опытная эксплуатация СЗРИ и СЗП в целях проверки их работоспособности	
	8	Участие в монтаже средств охраны и безопасности, инженерной защиты	
	9	Анализ уязвимости системы	
	10	Выявление ПЭМИН в информационной системе и защита от них	
	11	Восстановление информации при перехвате ПЭМИН	

	12	Предотвращение утечки информации через ПЭМИН ПК	
	13	Организационные мероприятия по технической защите информации от утечки по каналам ПЭМИН	
	14	Организационные мероприятия по технической защите информации в средствах вычислительной техники, автоматизированных системах и сетях от утечки по каналам ПЭМИН	
	15	Применение активных методов защиты информации от утечки по каналам ПЭМИН	
	16	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами	
	17	Оценка защищенности основных технических средств в составе автоматизированной системы от утечки информации по каналу побочных электромагнитных излучений	
	18	Оценка защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы от её утечки за счет наводок информативного сигнала	
	19	Участие в обслуживании технических средств защиты информации	
	20	Выполнение подбора, настройки и применения технических средств защиты информации	
	21	Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения	
	22	Использование средств охраны и безопасности объекта	
	23	Организация и реализация технической охраны объектов	
	24	Парольная аутентификация в системах ИБ и PIN-код в СКУД	
	25	Участие в организации работ по технической защите конфиденциальной информации	
	26	Контроль доступа к неструктурированным данным	
	27	Внутренний контроль обработки ПДн	
	28	Контроль за соответствием обработки ПДн	
	29	Участие в перехвате побочных электромагнитных излучений	
	30	Поиск и измерение ПЭМИ монитора на ЭЛТ (монитора на ЖК) в автоматическом и режиме управляющей программы	
	31	Составление протокол исследования с помощью расчетной программы	
	32	Съем наводок ПЭМИ ТСОИ с соединительных линий ВТСС и посторонних проводников	
	33	Защита информации в АСУ	
	34	Защита информации при передаче данных	
	35	Защита информации ограниченного доступа	
	36	Защита информации на жестком диске	
	37	Защита информации при использовании электронной почты	
	38	Комплексная защита информации в корпоративных системах	
	39	Защита информации в компьютерных сетях	

	40	Защита информации в локальных вычислительных сетях	
	41	Защита информации в VPN-сетях	
	42	Защита информации от несанкционированного доступа в сетях	
	43	Контроль доступа к информации	
	44	Управление доступом к информации	
	19	Участие в обслуживании технических средств защиты информации	
	20	Выполнение подбора, настройки и применения технических средств защиты информации	
	21	Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения	
	22	Использование средств охраны и безопасности объекта	
	23	Организация и реализация технической охраны объектов	
	24	Парольная аутентификация в системах ИБ и PIN-код в СКУД	
	25	Участие в организации работ по технической защите конфиденциальной информации	
	26	Контроль доступа к неструктурированным данным	
	27	Внутренний контроль обработки ПДн	
	28	Контроль за соответствием обработки ПДн	
	29	Участие в перехвате побочных электромагнитных излучений	
	30	Поиск и измерение ПЭМИ монитора на ЭЛТ (монитора на ЖК) в автоматическом и режиме управляющей программы	
	31	Составление протокол исследования с помощью расчетной программы	
	32	Съем наводок ПЭМИ ТСОИ с соединительных линий ВТСС и посторонних проводников	
	33	Защита информации в АСУ	
	34	Защита информации при передаче данных	
	35	Защита информации ограниченного доступа	
	36	Защита информации на жестком диске	
	37	Защита информации при использовании электронной почты	
	38	Комплексная защита информации в корпоративных системах	
	39	Защита информации в компьютерных сетях	
	40	Защита информации в локальных вычислительных сетях	
	41	Защита информации в VPN-сетях	
	42	Защита информации от несанкционированного доступа в сетях	
	43	Контроль доступа к информации	
	44	Управление доступом к информации	
	45	Техническая защита информации на предприятии	
	46	Инженерно-техническая защита информации на предприятии	

	47	Защита информации, составляющей коммерческую тайну	
	48	Разработка модели КСЗИ	
	49	Технологическое и организационное построение КСЗИ	
	50	Кадровое обеспечение функционирования КСЗИ	
	51	Участие в эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения	
	52	Участие в эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам	
	53	Установка и настройка средств защиты информации	
	54	Участие в монтаже технических средств защиты информации	
	55	Участие в монтаже средств охраны и безопасности, технической охраны объектов	
	56	Участие в монтаже средств защиты информации от несанкционированного съёма и утечки по техническим каналам	
	57	Настройка системы защиты информации от съёма и утечки по техническим каналам	
	58	Выявление технических каналов	
	59	Поиск ЗУ и других технических каналов	
	60	Выявление путей утечки информации в ИС	
	61	Оценка уязвимости системы	
	62	Участие в монтаже средств охраны и безопасности и систем видеонаблюдения	
	63	Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам	
	64	Определение требований к системе защиты информации	
	65	Проектирование системы защиты информации	
	66	Разработка эксплуатационной документации на систему защиты информации	
	67	Установка и настройка средств защиты информации	
	68	Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта	
	69	Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению	
	70	Испытания и опытная эксплуатации системы защиты информации	
	71	Подтверждение соответствия системы защиты информации	
	72	Выполнение мероприятий по предотвращению несанкционированного доступа к информации	
	73	Оценка эффективности использованных мер и средств защиты информации	
	74	Контроль эффективности защиты информации	

	75	Защита информации обрабатываемой ТСПИ от утечки по техническим каналам	
	76	Защита от утечки информации по телефонному каналу	
	77	Защита от утечки информации по электросетевому каналу	
	78	Защита от утечки информации по вибрационному каналу	
	79	Защита от утечки информации по проводному каналу	
	80	Формирование требований к системе защиты информации	
	81	Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности обрабатываемой информации	
	82	Изучение порядка применения нормативных правовых актов	
	83	Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами	
	84	Выявление технических каналов утечки информации	
	85	Применение существующих способов выявления опасности целостности информации	
	86	Анализ объектов информатизации предприятий, учреждений, организаций	
	87	Анализ ресурсов обеспечения инженерно-технической защиты информации	
	88	Изучение основных этапов проектирования системы защиты информации техническими средствами	
	89	Проектирование рабочих проектов по системе пожарно-охранной сигнализации, видеонаблюдения, СКУД	
	90	Оформление отчета	
Всего			108

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

3.1. Материально-техническое обеспечение

Производственная практика (по профилю специальности) проводится концентрированно после освоения всех разделов модуля. Базами производственной практики являются организации работодателей, с которыми заключены договоры о практической подготовке обучающихся:

Кабинет hr-бизнес-партнера

Липецкий филиал ПАО Ростелеком, 398000, Липецкая область, г. Липецк, ул. Валентины Терешковой, 35А, помещение 311, БТИ №5, 3 этаж, площадь 36 кв. м.

Рабочее место руководителя: стол, стул, ПК, подключённый в ЛВС с выходом в Интернет – 1 шт.

Рабочее место обучающегося: стол, стул, ПК, подключённый в ЛВС с выходом в Интернет – 10 шт.;

Источники бесперебойного питания – 10 шт.;

Многофункциональное устройство (МФУ) – 2 шт.

Обязательным условием допуска к производственной практике (по профилю специальности) в рамках профессионального модуля: ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты – является отсутствие у обучающихся академической задолженности по всем УД и ПМ.

Практика проводится под руководством преподавателей и специалистов предприятия-базы практики. Руководитель назначается приказом из числа преподавателей специальных дисциплин. В обязанности преподавателя-руководителя практики входит: контроль выполнения программы практики, оказание методической и практической помощи обучающему при отработке практических профессиональных умений и приобретения практического опыта, проверка заполнения дневника по производственной практике.

Руководители практики от предприятия-базы практик назначаются приказом руководителя предприятия до начала практики, из числа специалистов, имеющих образование, соответствующее профилю преподаваемого профессионального модуля.

Аттестация по итогам производственной практики (по профилю специальности) проводится на основании результатов, подтверждаемых отчётами и дневниками практики обучающихся, а также отзывами руководителей практики на обучающего.

Производственная практика (по профилю специальности) завершается зачётом обучающего освоенных общих и профессиональных компетенций.

Результаты прохождения производственной практики (по профилю специальности) учитываются при проведении государственной (итоговой) аттестации.

3.2. Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации имеет электронные издания и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Электронные издания:

1. Зверева, В. П. Технические средства информатизации : Учебник. - Москва: КУРС : ИНФРА-М, 2022. - 256 с. - (Среднее профессиональное образование). - ISBN 978-5-16- 105188-7. - Текст : электронный. - URL: <https://new.znaniy.com/catalog/product/1079430>
2. Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва : Издательство Юрайт, 2023. — 321 с. — (Профессиональное образование). — ISBN 978-5-534-07979-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://biblio-online.ru/bcode/442312>
3. Кузин, А. В. Компьютерные сети : учеб. пособие / А.В. Кузин, Д.А. Кузин. — 4-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2022. — 190 с. — (Среднее профессиональное образование). - ISBN 978-5-16-103935-9. - Текст : электронный. - URL: <https://new.znaniy.com/catalog/product/983172>

4. Миленина, С. А. Электротехника, электроника и схемотехника : учебник и практикум для среднего профессионального образования / С. А. Миленина, Н. К. Миленин ; под редакцией Н. К. Миленина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 406 с. — (Профессиональное образование). — ISBN 978-5-534-04676-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://www.biblio-online.ru/bcode/433455>
5. Шишмарёв, В. Ю. Электрорадиоизмерения. Практикум : практическое пособие для среднего профессионального образования / В. Ю. Шишмарёв. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 234 с. — (Профессиональное образование). — ISBN 978-5-534-08588-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://biblio-online.ru/bcode/441212>

В соответствии со ст. 43 Конституции Российской Федерации, 273-ФЗ «Об образовании в Российской Федерации» от 29.12.2012, приказом Минобрнауки России от 09.11.2015 N 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи», ГОСТ Р 57723-2017 «Информационно-коммуникационные технологии в образовании. Системы электронно-библиотечные. Общие положения», ГОСТ Р 52872-2019 «Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Приложения для стационарных и мобильных устройств, иные пользовательские интерфейсы. Требования доступности для людей с инвалидностью и других лиц с ограничениями жизнедеятельности», все предлагаемые электронные ресурсы максимально комфортны для чтения слабовидящими людьми. Масштабирование текста достигает 300 процентов. При изменении масштаба сохраняется возможность видеть всю страницу текста, не обрезая его.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Контроль и оценка результатов практики осуществляются с использованием следующих форм и методов: наблюдение за деятельностью студента на учебной практике, анализ документов, подтверждающих выполнение им соответствующих работ (например, отчет о практике, аттестационный лист, характеристика учебной и профессиональной деятельности студента, дневник прохождения практики). В результате прохождения учебной практики в рамках профессиональных модулей студенты проходят промежуточную аттестацию в форме дифференцированного зачета.

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в ИТКС	<ul style="list-style-type: none"> - проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации; 	Экспертное наблюдение
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в ИТКС	<ul style="list-style-type: none"> - проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации; 	Экспертное наблюдение
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями	<ul style="list-style-type: none"> - проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации; 	Экспертное наблюдение
ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС	<ul style="list-style-type: none"> - 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; 	Экспертное наблюдение

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;	Экспертное наблюдение
ОК 02.Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	Демонстрировать грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	Экспертное наблюдение
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	Экспертное наблюдение

учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения		
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	<ul style="list-style-type: none"> - эффективное выполнение правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности 	Экспертное наблюдение
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение