

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Карпова Елизавета Александровна  
Должность: директор  
Дата подписания: 13.05.2022 11:29:59  
Уникальный программный ключ:  
ad9053b6a9e639199a21a41d1a80dd3f5c40650966aaf85dff1ca3fca4a023d0



**СОЦИАЛЬНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ**  
**ЧАСТНОЕ УЧРЕЖДЕНИЕ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

**«УТВЕРЖДАЮ»**  
Директор ЧУ ПО «СТК»  
*Е. А. Карпова*  
«26» февраля 2021 г.

**ПРОГРАММА ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО)  
ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ  
ПРОГРАММЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА  
ПО СПЕЦИАЛЬНОСТИ**

**10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ**

**ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ  
ПМ.03. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-  
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С  
ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ**

**КВАЛИФИКАЦИЯ ВЫПУСКНИКА – ТЕХНИК ПО ЗАЩИТЕ ИНФОРМАЦИИ**

**Форма обучения:** очная

**Нормативный срок освоения программы –**

Уровень образования, необходимый для приема на обучение по ППССЗ	Срок получения СПО по ППССЗ базовой подготовки в очной форме обучения
среднее общее образование	2 года 10 месяцев

**Год начала подготовки:** 2021 год

**Тула, 2021**

Программа экзамена (квалификационного) составлена в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», зарегистрирован Министерством юстиции Российской Федерации от 26.12.2016г №44994.

Организация – разработчик:

Частное учреждение профессионального образования «Социально-технологический колледж»

Рабочая программа рассмотрена на заседании ПЦК (протокол № 1 от «20» февраля 2021г.) и признана соответствующей требованиям ФГОС СПО и учебного плана специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

Рабочая программа утверждена на заседании Педагогического совета («24» февраля 2021г., протокол № 2) и признана соответствующей требованиям ФГОС СПО специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

# Оглавление

I. ОБЩИЕ ПОЛОЖЕНИЯ .....	4
II. ЦЕЛИ И ЗАДАЧИ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО).....	5
III. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ .....	5
IV. СТРУКТУРА ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО) .....	16
V. УСЛОВИЯ ДОПУСКА К ЭКЗАМЕНУ (КВАЛИФИКАЦИОННОМУ) .....	16
VI. ПОРЯДОК ПРОВЕДЕНИЯ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО).....	16
VII. ФОРМА ПРОВЕДЕНИЯ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО).....	17
VIII. УКАЗАНИЯ ПО ФОРМЕ ПРОВЕДЕНИЯ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО).....	17
IX. ОБЩИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЭКЗАМЕНУ (КВАЛИФИКАЦИОННОМУ).....	19
X. ОЦЕНОЧНЫЕ СРЕДСТВА К ЭКЗАМЕНУ (КВАЛИФИКАЦИОННОМУ) ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ.....	20
XI. КРИТЕРИИ ОЦЕНКИ РЕЗУЛЬТАТОВ ОТВЕТОВ НА ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО).....	22
XII. МЕТОДИКА РАСЧЕТА БАЛЛЬНО-РЕЙТИНГОВОЙ ОЦЕНКИ ЗА ЭКЗАМЕН (КВАЛИФИКАЦИОННЫЙ) .....	23
XIII. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО), ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННО-СПРАВОЧНЫЕ СИСТЕМЫ.....	24
XIV. УЧЕБНАЯ ЛИТЕРАТУРА И РЕСУРСЫ СЕТИ ИНТЕРНЕТ, НЕОБХОДИМЫЕ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ (КВАЛИФИКАЦИОННОМУ) .....	25
XV. ОСОБЕННОСТИ ПРОВЕДЕНИЯ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО)ДЛЯ ЛИЦ С ОВЗ .....	25
XVI. ОБЩИЕ ПРАВИЛА ПОДАЧИ И РАССМОТРЕНИЯ АПЕЛЛЯЦИИ .....	32

## I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Программа разработана в соответствии со следующими нормативно-правовыми документами:

— Федеральным законом «Об образовании в Российской Федерации» №273-ФЗ от 29 декабря 2012 г. (с изменениями и дополнениями);

— Федеральными государственными образовательными стандартами среднего профессионального образования по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», реализуемом в частном учреждении профессионального образования «Социально-технологический колледж»

— Положение о фонде оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации в частном учреждении профессионального образования «Социально-технологический колледж»

— Положение об образовательной программе в частном учреждении профессионального образования «Социально-технологический колледж»

— Положение об экзамене (квалификационном) по итогам освоения профессионального модуля (вида профессиональной деятельности) программы среднего профессионального образования в соответствии с требованиями ФГОС;

— Положение о порядке и форме проведения государственной итоговой аттестации по программам подготовки специалистов среднего звена в частном учреждении профессионального образования «Социально-технологический колледж»;

1.2. Программа экзамена (квалификационного) по профессиональному модулю 03 «Защита информации в информационно-коммуникационных системах и сетях с использованием технических средств защиты» является частью основной профессиональной Образовательной программы по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

1.3. Экзамен (квалификационный) проводится после изучения междисциплинарных курсов (далее-МДК) модуля, прохождения учебной и производственной практики.

1.4. Итоговой формой контроля по профессиональному модулю 03 «Техническое обслуживание и ремонт компьютерных систем и комплексов» является квалификационный экзамен. Он проверяет готовность обучающегося к выполнению указанного вида профессиональной деятельности (далее – ВПД) и сформированность компетенций, определенных в разделе «Требования к результатам освоения основной профессиональной образовательной программы» (далее-ОПОП) федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 10.02.04 «Обеспечение информационной безопасности

телекоммуникационных систем». Итогом проверки является решение экзаменационной комиссии: «Вид профессиональной деятельности освоен / не освоен». Отметка определяется на основании подсчета общего количества баллов каждого эксперта, среднего балла всех экспертов, перевода балла в отметку в соответствии со шкалой перевода.

1.5. Промежуточная аттестация по профессиональному модулю 03 «Защита информации в информационно-коммуникационных системах и сетях с использованием технических средств защиты» осуществляется в форме экзамена (квалификационного) за счет времени, отведенного на промежуточную аттестацию.

1.6. Итоговая аттестация по профессиональному модулю — экзамен (квалификационный) проводится как процедура внешнего оценивания с участием представителей работодателя.

1.7. Целью проведения экзамена (квалификационного) является оценка соответствия достигнутых образовательных результатов, обучающихся по профессиональному модулю требованиям ФГОС СПО.

## **II. ЦЕЛИ И ЗАДАЧИ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО)**

Целью экзамена (квалификационного) является определение соответствия результатов освоения обучающимися образовательной программы требованиям ФГОС по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Задачей экзамена (квалификационного) является оценка степени и уровня освоения обучающимся профессионального, характеризующая его подготовленность к самостоятельному выполнению определенных видов профессиональной деятельности.

## **III. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

В результате изучения профессионального модуля ПМ. 03 «Защита информации в информационно-коммуникационных системах и сетях с использованием технических средств защиты» должен:

### **В ХОДЕ ОСВОЕНИЯ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ СТУДЕНТЫ ПРИОБРЕТАЮТ ПЕРВИЧНЫЙ ПРАКТИЧЕСКИЙ ОПЫТ:**

- установка, монтаж и настройка технических средств защиты информации;
- техническое обслуживание технических средств защиты информации;
- применение основных типов технических средств защиты информации;
- выявление технических каналов утечки информации;
- участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации;
- проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов

информатизации;

- проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;
- выявление технических каналов утечки информации;
- установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты.

**В ХОДЕ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ СТУДЕНТЫ ДОЛЖНЫ УМЕТЬ:**

- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
- применять технические средства для криптографической защиты информации конфиденциального характера;
- применять технические средства для уничтожения информации и носителей информации;
- применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;
- применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
- применять инженерно-технические средства физической защиты объектов информатизации.

**В ХОДЕ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ СТУДЕНТЫ ДОЛЖНЫ ЗНАТЬ:**

- порядок технического обслуживания технических средств защиты информации; - номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
- физические основы формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- структуру и условия формирования технических каналов утечки информации;
- порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;
- методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;
- номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;
- основные принципы действия и характеристики технических средств физической защиты;
- основные способы физической защиты информации;
- номенклатуру применяемых средств физической защиты объектов информатизации.

## **КОМПЕТЕНЦИИ, НЕОБХОДИМЫЕ ДЛЯ ПРОХОЖДЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ:**

Результатом освоения программы профессионального модуля является овладение студентами основных видов профессиональной деятельности (ВПД), профессиональных и общих компетенций.

Техник по компьютерным системам должен обладать **общими компетенциями**, включающими в себя способность:

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 9. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранных языках.

Техник по защите информации должен обладать **профессиональными компетенциями**, соответствующими основным видам профессиональной деятельности:

## **ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ**

ПК 3.1. Составлять схемы простых мехатронных систем в соответствии с техническим заданием.

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.



<b>ОБЩИЕ КОМПЕТЕНЦИИ</b>	
<b>Код и наименование компетенции</b>	<b>Виды профессиональной деятельности</b>
<p>ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.</p>	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- актуальный профессиональный и социальный контекст, в котором приходится работать и жить;</li> <li>- основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте.</li> <li>- алгоритмы выполнения работ в профессиональной и смежных областях;</li> <li>- методы работы в профессиональной и смежных сферах; структуру плана для решения задач;</li> <li>- порядок оценки результатов решения задач профессиональной деятельности.</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- распознавать задачу и/или проблему в профессиональном и/или социальном контексте;</li> <li>- анализировать задачу и/или проблему и выделять её составные части;</li> <li>- определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;</li> <li>- составить план действия;</li> <li>- определить необходимые ресурсы;</li> <li>- владеть актуальными методами работы в профессиональной и смежных сферах;</li> <li>- реализовать составленный план;</li> <li>- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)</li> </ul>
<p>ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.</p>	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- номенклатура информационных источников применяемых в профессиональной деятельности;</li> <li>- приемы структурирования информации;</li> <li>- формат оформления результатов поиска информации</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- определять задачи поиска информации;</li> <li>- определять необходимые источники информации;</li> <li>- планировать процесс поиска;</li> <li>- структурировать получаемую информацию; выделять наиболее значимое в перечне информации;</li> </ul>

	<ul style="list-style-type: none"> <li>- оценивать практическую значимость результатов поиска; оформлять результаты поиска</li> </ul>
<p>ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.</p>	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- содержание актуальной нормативно-правовой документации;</li> <li>- современную научную и профессиональную терминологию;</li> <li>- возможные траектории профессионального развития и самообразования</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- определять актуальность нормативно-правовой документации в профессиональной деятельности;</li> <li>- выстраивать траектории профессионального и личностного развития</li> </ul>
<p>ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.</p>	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- психология коллектива; психология личности;</li> <li>- основы проектной деятельности</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- организовывать работу коллектива и команды;</li> <li>- взаимодействовать с коллегами, руководством, клиентами</li> </ul>
<p>ОК 5. Осуществлять устную и письменную коммуникацию на</p>	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- особенности социального и культурного контекста;</li> </ul>

<p>государственном языке с учетом особенностей социального и культурного контекста.</p>	<p>- правила оформления документов.</p> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- излагать свои мысли на государственном языке;</li> <li>- оформлять документы.</li> </ul>
<p>ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.</p>	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- взаимосвязь общения и деятельности;</li> <li>- цели, функции, виды и уровни общения;</li> <li>- роли и ролевые ожидания в общении;</li> <li>- виды социальных взаимодействий;</li> <li>- механизмы взаимопонимания в общении;</li> <li>- техники и приемы общения, правила слушания, ведения беседы, убеждения;</li> <li>- этические принципы общения;</li> <li>- источники, причины, виды и способы разрешения конфликтов.</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- описывать значимость своей профессии</li> </ul> <p>Презентовать структуру профессиональной деятельности по профессии (специальности) ия.</p>
<p>ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.</p>	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности;</li> <li>- пути обеспечения ресурсосбережения.</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- соблюдать нормы экологической безопасности;</li> <li>- определять направления ресурсосбережения в рамках профессиональной деятельности по профессии (специальности).</li> </ul>
<p>ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания</p>	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- роль физической культуры в общекультурном, профессиональном и социальном развитии человека;</li> <li>- основы здорового образа жизни;</li> <li>- условия профессиональной деятельности и зоны риска физического здоровья для профессии (специальности); средства профилактики перенапряжения.</li> </ul>

<p>необходимого уровня физической подготовленности.</p>	<p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей;</li> <li>- применять рациональные приемы двигательных функций в профессиональной деятельности;</li> <li>- пользоваться средствами профилактики перенапряжения характерными для данной профессии (специальности)</li> </ul>
<p>ОК 9. Использовать информационные технологии в профессиональной деятельности.</p>	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- современные средства и устройства информатизации;</li> <li>- порядок их применения и программное обеспечение в профессиональной деятельности.</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- применять средства информационных технологий для решения профессиональных задач;</li> <li>- использовать современное программное обеспечение</li> </ul>
<p>ОК 10. Пользоваться профессиональной документацией на государственном и иностранных языках.</p>	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика);</li> <li>- лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности;</li> <li>- особенности произношения;</li> <li>- правила чтения текстов профессиональной направленности.</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы;</li> <li>- участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности;</li> <li>- кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы.</li> </ul>
<p><b>ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ</b></p>	

<p><b>ПК 3.1. Проводить контроль параметров, диагностику и восстановление работоспособности компьютерных систем и комплексов</b></p>	<p><b>Иметь практический опыт:</b></p> <ul style="list-style-type: none"> <li>- установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам;</li> </ul> <p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;</li> <li>- основные типы технических средств защиты информации от утечки по техническим каналам;</li> <li>- законодательства в области информационной безопасности, структуру государственной системы защиты информации, нормативных актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;</li> <li>- применять нормативные правовые акты и нормативные методические документы в области защиты информации;</li> </ul>
<p><b>ПК 3.2. Проводить системотехническое обслуживание компьютерных систем и комплексов</b></p>	<p><b>Иметь практический опыт:</b></p> <ul style="list-style-type: none"> <li>- установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам;</li> <li>- проведения технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;</li> </ul> <p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- основные типы технических средств защиты информации от утечки по техническим каналам;</li> <li>- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;</li> <li>- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;</li> </ul> <p><b>Уметь:</b></p>

	<ul style="list-style-type: none"> <li>- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;</li> <li>- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;</li> <li>- применять нормативные правовые акты и нормативные методические документы в области защиты информации;</li> </ul>
<p><b>ПК 3.3. Принимать участие в отладке и технических испытаниях компьютерных систем и комплексов, инсталляции, конфигурировании программного обеспечения</b></p>	<p><b>Иметь практический опыт:</b></p> <ul style="list-style-type: none"> <li>- защиты информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;</li> </ul> <p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;</li> <li>- основные типы технических средств защиты информации от утечки по техническим каналам;</li> <li>- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;</li> <li>- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС;</li> <li>- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;</li> <li>- применять нормативные правовые акты и нормативные методические документы в области защиты информации;</li> </ul>
<p><b>ПК 3.4. Производить восстановление и ремонт систем, программируемых контроллеров, периферийного оборудования и их</b></p>	<p><b>Иметь практический опыт:</b></p> <ul style="list-style-type: none"> <li>- проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;</li> <li>- выявление технических каналов утечки информации.</li> </ul>

<b>диагностирование с помощью тестовых программ и стендов</b>	<b>Знать:</b> - номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам. <b>Уметь:</b> - применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных.
---	---

#### **IV. СТРУКТУРА ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО)**

4.1. Экзамен проводится в форме:

— теоретического экзамена, содержащего вопросы по каждому междисциплинарному курсу входящему в профессиональный модуль, (форма проведения: устный экзамен);

— выполнения комплексного практического задания.

4.2. Оценка производится путём сопоставления усвоенных алгоритмов деятельности с заданным эталоном деятельности.

4.3. Задания для экзамена (квалификационного) ориентированы на проверку освоения компетенций внутри профессионального модуля.

4.4. Содержание заданий максимально приближено к ситуациям профессиональной деятельности.

#### **V. УСЛОВИЯ ДОПУСКА К ЭКЗАМЕНУ (КВАЛИФИКАЦИОННОМУ)**

Допуск к квалификационному экзамену студентов, обучающихся по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», осуществляется в соответствии с Положением об экзамене (квалификационном) по профессиональному модулю ЧУ ПО «СТК».

Условием допуска к экзамену (квалификационному) является успешное освоение обучающимися всех элементов программы профессионального модуля: теоретической части модуля (междисциплинарных курсов, далее – МДК) и практик (учебной и/или производственной в соответствии с программой профессионального модуля). По отдельным элементам программы профессионального модуля может проводиться промежуточная аттестация. Контроль освоения МДК и прохождения практики направлен на оценку результатов преимущественно теоретического обучения и практической подготовленности.

#### **VI. ПОРЯДОК ПРОВЕДЕНИЯ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО)**

6.1. Экзамен (квалификационный) проводится в специально подготовленных помещениях.

6.2. Для процедуры экзамена (квалификационного) по профессиональному модулю формируется специальная аттестационная комиссия.

6.3. В состав аттестационной комиссии включаются:

— председатель комиссии - представитель работодателя /



заместитель директора Колледжа по учебно-воспитательной работе или иное должностное лицо, утверждённое приказом по Колледжу;

- преподаватели профессионального модуля;
- представители работодателей;

6.4. В период подготовки к экзамену (квалификационному) проводятся консультации за счет общего бюджета времени, отведенного на консультации.

6.5. Студент допускается в помещение, где проводится экзамен (квалификационный) при наличии зачётной книжки.

## **VII. ФОРМА ПРОВЕДЕНИЯ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО)**

Экзамен (квалификационный) представляет собой выполнение комплексного практического задания и теоретического по каждому междисциплинарному курсу входящему в профессиональный модуль.

Экзамен (квалификационный) предназначен для контроля и оценки результатов освоения профессионального модуля 03 «Техническое обслуживание и ремонт компьютерных систем и комплексов» по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

## **VIII. УКАЗАНИЯ ПО ФОРМЕ ПРОВЕДЕНИЯ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО)**

Экзамен (квалификационный) проводится в устной форме по билетам. Каждый из билетов содержит по три теоретических вопроса, относящихся к одной из дисциплин, перечисленных в настоящей программы. Экзамен проводится в письменной и устной форме по вопросам, перечень которых прилагается. Время для подготовки к ответу – 1 академический час.

Проведение экзамена предполагает выступление студента перед экзаменационной комиссией в течение 10 – 15 минут по вопросам, сформулированным в билете.

Экзаменаторам предоставляется право задавать студентам дополнительные вопросы в соответствии с утвержденной программой. Присутствие посторонних лиц на государственных экзаменах допускается только с разрешения ректора вуза.

Экзамен (квалификационный) проводится с целью контроля выполнения требований к уровню подготовки студентов и подтверждения их соответствия квалификационной характеристике и требованиям к профессиональной подготовленности бакалавра, изложенным в государственном образовательном стандарте. Перед экзаменом проводятся

обзорные лекции по дисциплинам, вопросы по которым включаются в экзаменационные билеты.

Всего на экзамен выносятся 30 билетов, в каждом билете по три вопроса. На экзамене студенты получают Программу экзамена.

Процедура проведения экзамена (квалификационного) состоит из следующих этапов:

#### 1. Начало экзамена.

Перед началом экзамена студенты – выпускники приглашаются в аудиторию. Председатель знакомит присутствующих с приказом о создании комиссии по проведению экзамена (квалификационного): зачитывает его и представляет состав экзамена (квалификационного) персонально. Затем вскрывается конверт с экзаменационными билетами, проверяется их количество. Все экзаменационные билеты раскладываются на столе.

В аудитории остаются пять - шесть выпускников, остальные покидают аудиторию. Студенты берут билет, называют его номер и занимают индивидуальное место за столом для подготовки ответов. На подготовку к ответу студентам отводится 1 час.

#### 2. Заслушивание ответов.

Студент отвечает на все вопросы билета, а затем по ним могут быть заданы уточняющие, поясняющие, дополняющие вопросы. Как правило, дополнительные вопросы тесно связаны с основными вопросами билета. Право выбора порядка ответа предоставляется отвечающему студенту.

Комиссия дает ему возможность дать полный ответ по всем вопросам. В некоторых случаях по инициативе председателя, заместителя или членов комиссии (или в результате их согласованного решения) ответ студента может быть тактично приостановлен. При этом дается краткое, но убедительное пояснение причины:

1) ответ явно не по существу вопроса, ответ слишком детализирован, студент допускает явную ошибку в изложении нормативных актов, статистических данных;

2) студент грамотно и полно изложил основное содержание вопроса, но продолжает его развивать. Если ответ остановлен по первой причине, то студенту предлагается перестроить содержание излагаемой информации сразу же или после ответа на другие вопросы билета.

По итогам проведения экзамена комиссия делает вывод об усвоении студентом соответствующих компетенций и выставляет итоговую оценку: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Все студенты, сдававшие экзамен в соответствующий день, приглашаются в аудиторию, где работает экзамена (квалификационного).

Председатель экзамена (квалификационного) сообщает, что в результате обсуждения и совещания оценки выставлены, и оглашает их. Отмечает лучших обучающихся, высказывает общие замечания. Обращается к студентам, нет ли не согласных с решением комиссии по оценке ответа.

Результаты выставленных оценок (и их мотивация) оглашаются открыто в присутствии всей группы обучающихся, участвовавших на публичном экзамене. Выставленные оценки при необходимости комментируются

Председателем комиссии экзамена (квалификационного) в присутствии всех аттестуемых студентов. В случае несогласия с оценкой, студент об этом может заявить в письменной форме (заявление) в комиссию на имя председателя. Заявление рассматривается на этом же заседании по материалам ответа студента при прохождении испытания. Оценки по каждому студенту заносятся в протоколы и зачетные книжки, комиссия подписывает эти документы.

Студент, имеющий неудовлетворительную оценку по экзамену (квалификационному), имеет право на пересдачу согласно графика учебного процесса колледжа.

На каждого студента заполняется протокол приема экзамена (квалификационного), в который вносятся вопросы билетов и дополнительные вопросы членов экзамена (квалификационного). Протокол приема экзамена (квалификационного) подписывается теми членами экзамена (квалификационного), которые присутствовали на экзамене.

Подведение итогов работы экзамена (квалификационного).

По завершении экзамена (квалификационного) председатель комиссии экзамена (квалификационного) готовит письменный отчет, в котором приводятся статистические данные о количестве обучающихся, сдававших экзамен, отмечается уровень знаний и делаются предложения кафедрам по совершенствованию преподавания отдельных дисциплин.

## **IX. ОБЩИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЭКЗАМЕНУ (КВАЛИФИКАЦИОННОМУ)**

Обучающийся должен самостоятельно изучить или обновить полученные ранее знания, умения, навыки, характеризующие практическую и теоретическую подготовленность по темам, содержание которых составляет предмет государственного экзамена (итогового экзамена) и соответствует требованиям по готовности к видам профессиональной деятельности, решению профессиональных задач (и освоению компетенций), перечисленных в п. 2 настоящей программы.

Перед государственным междисциплинарным экзаменом проводятся консультации по вопросам, включенным в данную программу.

Рекомендации: при подготовке к экзамену желательно составлять конспекты, иллюстрируя отдельные прорабатываемые вопросы. Материал должен конспектироваться кратко, четко, конкретно в рамках обозначенной темы.

## **Х. ОЦЕНОЧНЫЕ СРЕДСТВА К ЭКЗАМЕНУ (КВАЛИФИКАЦИОННОМУ) ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ**

### **ЗАДАНИЯ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ**

#### **Теоретические вопросы**

1. Средства информации как предмета защиты техническими средствами.
2. Демаскирующие признаки объектов защиты, сигналов, веществ.
3. Носители и источники информации. Запись и съем информации с ее носителя.
4. Источники угроз безопасности информации.
5. Опасные сигналы и их источники.
6. Виды угроз безопасности информации, защищаемой техническими средствами. Органы добывания информации. Технология добывания информации.
7. Добывание информации без физического проникновения в контролируемую зону. Способы несанкционированного доступа к источнику информации. Способы и средства добывания информации техническими средствами. Способы и средства перехвата сигналов.
8. Классификация и структура технических каналов утечки информации. Акустические каналы утечки.
9. Оптические каналы утечки. Радиоэлектронные каналы утечки информации. Вещественные каналы утечки информации.
10. Концепция инженерно-технической защиты информации.
11. Факторы обеспечения защиты информации от физической защиты информации. Способы и средства защиты информации от наблюдения.
12. Методы противодействия радиолокальному и гидроакустическому наблюдению.
13. Методы противодействия подслушиванию.
14. Способы и средства предотвращения утечки информации через ПЭМИН. Способы предотвращения утечки информации по материально-вещественному каналу. Защита объектов от химической, радиационной и магнитометрической разведок, системы защиты от утечки информации по электросетевому каналу, моделирование объектов защиты и каналов утечки информации.
15. Инженерно-техническая защита информации.
16. Характеристика средств технической разведки. Возможности средств технической разведки.
17. Акустические приемники. Диктофоны. Закладные устройства. Лазерные средства подслушивания.

18. Средства перехвата радиосигналов. Технические средства анализа сигналов.
19. Средства определения координат источников радио сигналов и перехвата оптических и электрических сигналов. Определение координат источников радиоизлучений и анализа сигналов.
20. Способы и средства уничтожения информации. Способы и средства стирания информации на магнитных носителях.
21. Средства инженерной защиты. Инженерные конструкции.
22. Ограждение территорий, зданий, помещений. Двери, окна, Ворота. Металлические сейфы, хранилища. Запирающие устройства.
23. Подходы к проектированию систем защиты информации. Принципы построения системы защиты информации.
24. Методологические основы системы защиты информации. Методика определения состава защищаемой информации. Выявление каналов доступа к информации.
25. Определение источников дестабилизирующего воздействия на информацию.
26. Понятие модели объекта. Технологическое построение системы защиты информации.
27. Кадровое обеспечение защиты информации.
28. Кодекс корпоративного поведения.
29. Нормативно-методическое обеспечение защиты информации. Управление системой защиты информации. Разработка системы ИТЗИ. Построение системы безопасности предприятия.
30. Виды, методы и погрешности.
31. Классификация измерительных приборов.
32. Амперметры и вольтметры. Включение их в цепь.
33. Генераторы измерительные.
34. Генераторы шума.
35. Универсальные осциллографы.
36. Способы отсчета напряжения и временных интервалов электрических сигналов.
37. Методы измерения частоты и временных интервалов электрических сигналов.
38. Измерение параметров с сосредоточенными параметрами.
39. Измерение АЧХ.
40. Измерение параметров полупроводниковых приборов.

### **Практические задания**

1. Маскировка в видимом и ИК диапазонах света.
2. Активное подавление сигналов радиолокатора.

3. Энергетическое скрывание акустических сигналов: звукоизоляция и звукопоглощение.
4. Определение погрешности измерений.
5. Измерение параметров электрической цепи комбинированным прибором.
6. Измерение напряжений цифровым вольтметром.
7. Исследование органов управления, включение и калибровки электронного осциллографа.
8. Измерение параметров различных сигналов двухканальным осциллографом.
9. Настройка системы защиты информации от съема и утечки по техническим каналам.
10. Выявление технических каналов утечки информации.
11. Проектирование рабочих проектов по системе пожарно-охранной сигнализации, видеонаблюдения, СКУД.
12. Измерение мощности и силы постоянного электромагнитного тока.
13. Измерение постоянного напряжения методом компенсации.
14. Измерение переменного электрического напряжения.
15. Измерение частоты и периода электрических сигналов.
16. Измерение токов, напряжений и сопротивлений, исследование двухполюсников с помощью мультиметра.
17. Обработка и представление однократных измерений при наличии систематической погрешности.

## **XI. КРИТЕРИИ ОЦЕНКИ РЕЗУЛЬТАТОВ ОТВЕТОВ НА ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО)**

Оценка ответа обучающегося определяется в ходе заседания экзамена (квалификационного) по приему экзамена (квалификационного). Балльно-рейтинговая оценка по экзамену (квалификационному) отражает уровень продемонстрированных знаний, аргументированность и полноту ответов на вопросы комиссии.

Экзамен (квалификационный) оценивается по 100-балльной шкале.

<b>Государственный экзамен (квалификационный)</b>	<b>Количество баллов</b>
Председатель комиссии	0-20
Зам. председателя комиссии	0-20
Член комиссии	0-20
Член комиссии	0-20

Член комиссии	0-20
<b>Итого</b>	<b>0-100</b>

## XII. МЕТОДИКА РАСЧЕТА БАЛЛЬНО-РЕЙТИНГОВОЙ ОЦЕНКИ ЗА ЭКЗАМЕН (КВАЛИФИКАЦИОННЫЙ)

Балльно-рейтинговая оценка за экзамен (квалификационный), выставляемая каждым членом комиссии, может быть рассчитана на основании следующих критериев.

№ вопроса	Уровень готовности		
	Критический	Допустимый	Оптимальный
1	Обучающийся слабо демонстрирует свою достаточно осведомленность в нормативно-правовой базе по основным дисциплинам, общие знания поверхностные и неглубокие, слабо владеет научной терминологией и понятийным аппаратом 20 - 25	Обучающийся демонстрирует свою среднюю осведомленность в нормативно-правовой базе по основным дисциплинам, есть но не совсем глубокие и всесторонние знания, владеет, но не свободно научной терминологией и понятийным аппаратом 25 - 30	Обучающийся демонстрирует свою достаточно высокую осведомленность в нормативно-правовой базе по основным дисциплинам, глубокие и всесторонние знания, свободно владеет научной терминологией и понятийным аппаратом. 30 - 35
2	Обучающийся слабо ориентируется в теоретическом материале, слабо анализирует различные концепции, модели, не сравнивает их, не приводит убедительные аргументы, в возможностях их использования в профессиональной деятельности 20 - 25	Обучающийся ориентируется, но не уверенно в теоретическом материале, пытается анализировать различные концепции, модели, сравнивает их, пытается приводить убедительные аргументы, в возможностях их использования в профессиональной деятельности 25-30	Обучающийся свободно ориентируется в теоретическом материале, анализирует различные концепции, модели, сравнивает их, приводит убедительные аргументы, в возможностях их использования в профессиональной деятельности. 30 - 35

3	<p>Ответ (решение задачи) не структурирован. Обучающийся слабо и неуверенно отвечает на дополнительные вопросы 10 - 20</p>	<p>Ответ (решение задачи) средне структурирован. Обучающийся пытается осознанно и точно отвечать на дополнительные вопросы 21- 25</p>	<p>Ответ (решение задачи) хорошо структурирован. Обучающийся осознанно, уверенно и точно отвечает на дополнительные вопросы 26 - 30</p>
	50-70	71-91	92-100

Результаты решения ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО) могут определяться оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Балльно-рейтинговая оценка по ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО) выставляется в соответствии со следующей шкалой:

50–70 – «удовлетворительно»;

71–91 – «хорошо»;

92–100 – «отлично».

Далее приводятся критерии оценки результатов ответов. Например:

Оценка "ОТЛИЧНО" ставится обучающемуся, показавшему повышенный уровень готовности к профессиональной деятельности

Оценка "ХОРОШО" ставится обучающемуся, показавшему пороговый (допустимый) уровень готовности к профессиональной деятельности.

Оценка "УДОВЛЕТВОРИТЕЛЬНО" ставится обучающемуся, показавшему пороговый (критический) уровень готовности к профессиональной деятельности.

Оценка "НЕУДОВЛЕТВОРИТЕЛЬНО" ставится обучающемуся, не достигшему пороговый уровень готовности к профессиональной деятельности.

### **ХIII. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО), ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННО-СПРАВОЧНЫЕ СИСТЕМЫ**

Информационные технологии обработки графической информации; информационные технологии передачи данных и распространения информации; информационные технологии хранения данных; информационные технологии накопления данных. Сетевые (локальные, территориальные, проводные, беспроводные и др.) информационные технологии, информационные технологии групповой работы, гипертекстовые информационные технологии, мультимедийные



информационные технологии, операционные системы семейства Windows, Office, браузеры (FireFox);

базы данных, информационно-справочные и поисковые системы: доступ к базам РГБ, ГНБУ, ERIC ([www.rsl.ru](http://www.rsl.ru), [www.gnpbu.ru](http://www.gnpbu.ru)), Министерства образования и науки Российской Федерации ([www.informica.ru](http://www.informica.ru)), научная электронная библиотека <http://elibrary.ru/>.

#### **XIV. УЧЕБНАЯ ЛИТЕРАТУРА И РЕСУРСЫ СЕТИ ИНТЕРНЕТ, НЕОБХОДИМЫЕ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ (КВАЛИФИКАЦИОННОМУ)**

##### **ОСНОВНЫЕ ИСТОЧНИКИ**

1. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябов Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2016. – 363 с.
2. Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов, 5-е изд. – СПб.: Питер, 2015. – 944 с.
3. Томаси У. Электронные системы связи. - М.: Техносфера, 2016. -1360с.
4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: в 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.
5. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: в 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2013. – 172 с.
6. Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с
7. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012
8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012
9. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник: Рекомендовано УМО, 2009. - 192с.
10. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

##### **ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ**

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
- Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
- Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
- Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
- Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
- Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
- Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
- Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
- Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической

- защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
- Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
  - Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
  - Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
  - Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
  - Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
  - Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
  - Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
  - Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
  - ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
  - ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

- ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
- ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
- ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
- ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
- ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
- ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
- ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
- ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
- ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
- ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
- ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
- ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от

- преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
- ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
  - ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
  - ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
  - Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
  - Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
  - ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
  - Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
  - Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
  - Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

#### **Отечественные журналы:**

"InformationSecurity/ Информационная безопасность".

Системный администратор.

Компьютер ПРЕСС.

Системы безопасности. Журнал для руководителей и специалистов в области безопасности.

Сети и системы связи.

Защита информации. Инсайд: Информационно-методический журнал.

Информационная безопасность регионов: Научно-практический журнал.

#### ИНТЕРНЕТ\_РЕСУРСЫ

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [www.fstec.ru](http://www.fstec.ru)

Информационно-справочная система по документам в области технической защиты информации [www.fstec.ru](http://www.fstec.ru)

Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>

Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>

<http://www.morion.ru/>

<http://www.nateks.ru/>

<http://www.iskratel.com/>

<http://www.ps-ufa.ru/>

<http://3m.com/>

<http://www.rusgates.ru/index/php> - Материалы сайта завода «Ферроприбор»

#### **XV. [HTTP://CRYPTOGROF.RU/](http://CRYPTOGROF.RU/) ОСОБЕННОСТИ ПРОВЕДЕНИЯ ЭКЗАМЕНА (КВАЛИФИКАЦИОННОГО) ДЛЯ ЛИЦ С ОВЗ**

Для обучающихся из числа инвалидов экзамен (квалификационный) проводится в ЧУ ПО «СТК» с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья (далее - индивидуальные особенности).

При проведении экзамена (квалификационного) обеспечивается соблюдение следующих общих требований:

Проведение экзамена (квалификационного) для инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при прохождении экзамена (квалификационного);

Присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с председателем и членами экзамена (квалификационного));

Пользование необходимыми обучающимся инвалидам техническими

средствами при прохождении экзамена (квалификационного с учетом их индивидуальных особенностей);

Обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже, наличие специальных кресел и других приспособлений).

Все локальные нормативные акты ЧУ ПО «СТК» по вопросам проведения экзамена (квалификационного) доводятся до сведения обучающихся инвалидов в доступной для них форме.

По письменному заявлению обучающегося инвалида продолжительность сдачи обучающимся инвалидом экзамена (квалификационного) может быть увеличена по отношению к установленной продолжительности его сдачи:

Продолжительность сдачи экзамена (квалификационного), проводимого в письменной форме, - не более чем на 90 минут;

Продолжительность подготовки обучающегося к ответу на экзамене (квалификационном), проводимом в устной форме, - не более чем на 20 минут;

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья организация обеспечивает выполнение следующих требований при проведении экзамена (квалификационного):

А) для слепых:

Задания и иные материалы для сдачи экзамена (квалификационного) оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом;

Письменные задания выполняются обучающимися на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых, либо надиктовываются ассистенту;

При необходимости обучающимся предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

Б) для слабовидящих:

Задания и иные материалы для сдачи государственного аттестационного испытания оформляются увеличенным шрифтом;

Обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

При необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств,

имеющихся у обучающихся;

В) для глухих и слабослышащих, с тяжелыми нарушениями речи:

Обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования;

По их желанию государственные аттестационные испытания (итоговые аттестационные испытания) проводятся в письменной форме;

Г) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

Письменные задания выполняются обучающимися на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

По их желанию государственные аттестационные испытания проводятся в устной форме.

Обучающийся инвалид не позднее чем за 3 месяца до начала проведения экзамена (квалификационного) подает письменное заявление о необходимости создания для него специальных условий при проведении государственных аттестационных испытаний с указанием его индивидуальных особенностей. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).

В заявлении обучающийся указывает на необходимость (отсутствие необходимости) присутствия ассистента на экзамене (квалификационном), необходимость (отсутствие необходимости) увеличения продолжительности сдачи государственного аттестационного испытания по отношению к установленной продолжительности.

## **XVI. ОБЩИЕ ПРАВИЛА ПОДАЧИ И РАССМОТРЕНИЯ АПЕЛЛЯЦИИ**

По результатам государственных аттестационных испытаний обучающийся имеет право на апелляцию.

Обучающийся имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению, установленной процедуры проведения государственного аттестационного испытания и (или) несогласии с результатами государственного экзамена.

Председателем апелляционной комиссии утверждается ректор (лицо, исполняющее его обязанности, или лицо, уполномоченное руководителем организации - на основании распорядительного акта).

В состав апелляционной комиссии входят председатель указанной комиссии и не менее 3 членов указанной комиссии. Состав апелляционной



комиссии формируется из числа лиц, относящихся к профессорско-преподавательскому составу организации и не входящих в состав государственных экзаменационных комиссий.

Апелляция подается лично обучающимся в апелляционную комиссию не позднее следующего рабочего дня после объявления результатов экзамена (квалификационного).

Для рассмотрения апелляции секретарь экзамена (квалификационного) направляет в апелляционную комиссию протокол заседания экзамена (квалификационного), заключение председателя экзамена (квалификационного) о соблюдении процедурных вопросов при проведении государственного аттестационного испытания, а также письменные ответы обучающегося (при их наличии) (для рассмотрения апелляции по проведению государственного экзамена) либо выпускную квалификационную работу, отзыв и рецензию (рецензии) (для рассмотрения апелляции по проведению защиты выпускной квалификационной работы).

Апелляция не позднее 2 рабочих дней со дня ее подачи рассматривается на заседании апелляционной комиссии, на которое приглашаются председатель государственной экзаменационной комиссии и обучающийся, подавший апелляцию. Заседание апелляционной комиссии может проводиться в отсутствие обучающегося, подавшего апелляцию, в случае его неявки на заседание апелляционной комиссии.

Решение апелляционной комиссии доводится до сведения обучающегося, подавшего апелляцию, в течение 3 рабочих дней со дня заседания апелляционной комиссии. Факт ознакомления обучающегося, подавшего апелляцию, с решением апелляционной комиссии удостоверяется подписью обучающегося.

При рассмотрении апелляции о нарушении процедуры проведения государственного аттестационного испытания апелляционная комиссия принимает одно из следующих решений:

об отклонении апелляции, если изложенные в ней сведения о нарушениях процедуры проведения государственного аттестационного испытания (итогового аттестационного испытания) обучающегося не подтвердились и (или) не повлияли на результат государственного аттестационного испытания;

об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях процедуры проведения государственного аттестационного испытания (итогового аттестационного испытания) обучающегося подтвердились и повлияли на результат государственного аттестационного испытания.

В случае, если результат проведения государственного аттестационного испытания (итогового аттестационного испытания) подлежит аннулированию, в связи с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в государственную

экзаменационную комиссию для реализации решения апелляционной комиссии. Обучающемуся предоставляется возможность пройти государственное аттестационное испытание в сроки, установленные образовательной организацией.

При рассмотрении апелляции о несогласии с результатами экзамена (квалификационного) апелляционная комиссия выносит одно из следующих решений:

об отклонении апелляции и сохранении результата государственного экзамена;

об удовлетворении апелляции и выставлении иного результата государственного экзамена.

Решение апелляционной комиссии не позднее следующего рабочего дня передается в комиссию экзамена (квалификационного). Решение апелляционной комиссии является основанием для аннулирования ранее выставленного результата государственного экзамена и выставления нового.

Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

Повторное проведение экзамена (квалификационного) обучающегося, подавшего апелляцию, осуществляется в присутствии председателя или одного из членов апелляционной комиссии не позднее даты завершения обучения в организации в соответствии со стандартом.

Апелляция на повторное проведение экзамена (квалификационного) не принимается.