**МИНИСТЕРСТВО ОБРАЗОВАНИЯ КРАСНОЯРСКОГО КРАЯ**

**Краевое государственное бюджетное профессиональное образовательное учреждение**
**«КРАСНОЯРСКИЙ МОНТАЖНЫЙ КОЛЛЕДЖ»**

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

для профессионального модуля **ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи**

по специальности **11.02.15 Инфокоммуникационные сети и системы связи**

г. Красноярск
2023

СОГЛАСОВАНО

Генеральный директор
АО КПМФ «Востокпромсвязьмонтаж»
_____ В.В. Поткин
«15» 02 2023 г.

УТВЕРЖДАЮ

Заместитель директора по
учебно-производственной работе
_____ А.О. Растащёнов

Программа учебной практики для ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи составлена в соответствии с требованиями ФГОС СПО по специальности 11.02.15 Инфокоммуникационные сети и системы связи, утверждённого приказом Министерства просвещения РФ от «05» августа 2022 г. №675.

ОДОБРЕНА
предметной (цикловой) комиссией
специальности «ССиСК»

протокол № 5 от 19.01 2023г.

Председатель ПЦК _____ И.В. Селина

Разработчик:
преподаватель КГБПОУ
«Красноярский монтажный колледж» _____ И.В. Селина

# СОДЕРЖАНИЕ

# 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

## 1.1. Область применения программы

Рабочая программа учебной практики является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 11.02.15 Инфокоммуникационные сети и системы связи, утвержденного приказом Министерства просвещения РФ от 05 августа 2022 г. № 675, входящей в укрупненную группу специальностей 11.00.00 Электроника, радиотехника и системы связи.

Рабочая программа составлена для учебной практики по профессиональному модулю ПМ.01 Техническая эксплуатация информационно-коммуникационных сетей связи.

Рабочая программа разработана на основе примерной основной образовательной программы подготовки специалистов среднего звена специальности 11.02.15 Инфокоммуникационные сети и системы связи, организация разработчик: Государственное бюджетное профессиональное образовательное учреждение города Москвы «Колледж связи № 54 им. П.М. Вострухина» (ГБПОУ КС №54).

Учебная практика направлена на комплексное освоение обучающимися всех видов профессиональной деятельности по специальности, формирование общих и профессиональных компетенций, приобретение необходимых умений и опыта практической работы по специальности.

Программа учебной практики УП.03.01 составлена для выполнения части практических занятий с целью освоения практического опыта, умений и знаний по МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи.

## 1.2. Место учебной практики в структуре основной профессиональной образовательной программы

Учебная практика входит в общепрофессиональный цикл профессиональной подготовки соответствующего профессионального модуля. Практике предшествует изучение МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи.

## 1.3. Цели и задачи учебной практики – требования к результатам освоения практических занятий

Цели и задачи учебной практики – это комплексное освоение обучающимися вида профессиональной деятельности ВД.3 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи по специальности, формирование общих и профессиональных компетенций, приобретение необходимых умений, знаний и опыта практической работы по специальности, в том числе:

| | |
|---|---|
| **Иметь практический опыт (ПО.1-ПО.5)** | – ПО.1 анализировать сетевую инфраструктуру;<br>– ПО.2 выявлять угрозы и уязвимости в сетевой инфраструктуре;<br>– ПО.3 разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи;<br>– ПО.4 осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи;<br>– ПО.5 использовать специализированное программное обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи; |
| **Уметь (У.1-У.14)** | – У.1 классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;<br>– У.2 проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;<br>– У.3 определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;<br>– У.4 осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки; |

| | |
|---|---|
| | – У.5 выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты;<br>– У6. выполнять тестирование систем с целью определения уровня защищенности, определять оптимальные способы обеспечения информационной безопасности;<br>– У.7 проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;<br>– У.8 проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;<br>– У.9 разрабатывать политику безопасности сетевых элементов и логических сетей;<br>– У.10 выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;<br>– У.11 производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;<br>– У.12 конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;<br>– У.13 защищать базы данных при помощи специализированных программных продуктов;<br>– У.14 защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами |
| **Знать (З.1–З.21)** | – З.1 принципы построения информационно-коммуникационных сетей;<br>– З.2 международные стандарты информационной безопасности для проводных и беспроводных сетей;<br>– З.3 нормативно-правовые и законодательные акты в области информационной безопасности;<br>– З.4 акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;<br>– З.5 технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;<br>– З.6 способы и методы обнаружения средств съёма информации в радиоканале;<br>– З.7 классификацию угроз сетевой безопасности;<br>– З.8 характерные особенности сетевых атак;<br>– З.9 возможные способы несанкционированного доступа к системам связи,<br>– З.10 правила проведения возможных проверок согласно нормативным документам ФСТЭК;<br>– З.11 этапы определения конфиденциальности документов объекта защиты;<br>– З.12 назначение, классификацию и принципы работы специализированного оборудования;<br>– З.13 методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;<br>– З.14 методы и средства защиты информации в телекоммуникациях от вредоносных программ;<br>– З.15 технологии применения программных продуктов;<br>– З.16 возможные способы, места установки и настройки программных продуктов,<br>– З.17 методы и способы защиты информации, передаваемой по кабельным направляющим системам;<br>– З.18 конфигурации защищаемых сетей; |

| | |
|---|---|
| | – З.19 алгоритмы работы тестовых программ;<br>– З.20 средства защиты различных операционных систем и среды передачи информации;<br>– З.21 способы и методы шифрования (кодирование и декодирование) информации. |

**1.4. Количество часов на освоение программы учебной практики:**

Обязательная учебная нагрузка обучающегося – 36 часов (1 неделя).

Промежуточная аттестация проводится в форме *дифференцированного зачёта*.

# 2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения рабочей программы учебной практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках модулей ОПОП СПО по основному виду профессиональной деятельности (ВПД) ВПД.3 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Общие компетенции:

| Код | Наименование общих компетенций |
|---|---|
| **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 личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по 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 общечеловеческих 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 08.** | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности |
| **ОК 09.** | Пользоваться профессиональной документацией на государственном и иностранном языках |

Профессиональные компетенции:

| Код | Наименование видов деятельности и профессиональных компетенций |
|---|---|
| **ВПД 3** | Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи |
| **ПК 3.1.** | Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности |
| **ПК 3.2.** | Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи |
| **ПК 3.3.** | Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования |

## 3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

### 3.1. Тематический план учебной практики

| Код и наименование учебной практики | Коды общих и профессиональных компетенций | Наименования разделов учебной практики | Объем часов |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **УП.03.01** | **ОК 01. – ОК 09.<br>ПК 3.1 – ПК 3.3** | **Раздел 1 Защита информации в инфокоммуникационных системах и сетях связи** | **36** |
| **Всего:** | | | **36** |

## 3.2. Содержание обучения по учебной практике

| Код и наименование профессионального модуля, МДК и тем учебной практики | Содержание учебных занятий | Объем часов на учебную практику |
|---|---|---|
| 1 | 2 | 3 |
| **Раздел 1 Защита информации в инфокоммуникационных системах и сетях связи** | | **36** |
| **Тема 1. Реализация политик безопасности в системах и сетях на примере дискреционной модели с использованием автоматизированной матрицы доступа (например, Power.Matrix).** | **Содержание** | **6** |
| | Применение избирательной (дискреционной) политики безопасности. | 6 |
| | Применение матрицы доступа для описания избирательных свойств управления доступом. | |
| | Автоматизация задачи учета пользователей и их полномочий в инфраструктуре с помощью (например, Power.Matrix). | |
| **Тема 2. Проведение анализа рисков информационной безопасности при построении системы защиты в соответствии с международным стандартом информационной безопасности ISO 17799.** | **Содержание** | **6** |
| | Применение программного комплекса анализа и контроля рисков информационных систем компании ГРИФ. | 6 |
| | Применение программного комплекса управления политикой информационной безопасности компании Кондор+. | |
| | Определение источников угроз. | |
| | Оценка рисков по двум и трем факторам. | |
| **Тема 3. Проведение анализа защищенности объекта защиты информации.** | **Содержание** | **6** |
| | Классификация каналов несанкционированного получения информации. | 6 |
| | Причины нарушения целостности информации. | |
| | Архитектура системы защиты информации (ядро, ресурсы, организационное построение. | |
| | Анализ увеличения защищенности объекта защиты информации. | |
| **Тема 4. Проведение инструментальных проверок объекта защиты информации.** | **Содержание** | **6** |
| | Проведение активного аудита информационной безопасности. | 6 |
| | Постановка задачи для проведения инструментальных проверок. | |
| | Обнаружение сетевых узлов. | |
| **Тема 5. Сканирование портов, идентификация ОС, использование DNS для обнаружения и выяснения назначения сетевых узлов при проведении инструментальной проверки** | **Содержание** | **6** |
| | Обнаружение открытых TCP– и UDP–портов на обнаруженных узлах путем сканирования портов. | 6 |
| | Получение DNS–имен сетевых узлов. | |
| | Получение списка сетевых узлов организации, а также информации об их назначении с применением переноса зоны DNS. | |
| | Построение карты сети. | |
| | 5.5 Идентификация ОС и ПО путем получения «отпечатков ОС». | |

| | | |
|---|---|---|
| **Тема 6. Использование сканера безопасности Nessus для выявления уязвимостей систем и сетей.** | **Содержание** | **6** |
| | 6.1 Установка сканера безопасности Nessus на виртуальную машину и тестирование наличия уязвимостей на узлах исследуемой сети. | 6 |
| | 6.2 Использование анализатора сетевого трафика для сканирования сети с целью получения представления о том, какая информация циркулирует в сети. | |
| | 6.3 Использование системы обнаружения атак для установления факта сканирования сети. | |
| | 6.4 Оформление перечня найденных уязвимостей | |
| **Всего** | | **36** |

# 4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

### 4.1. Требования к минимальному материально-техническому обеспечению

Учебная практика профессионального модуля ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи по профилю специальности 11.02.15 Инфокоммуникационные сети и системы связи проходит на базе КГБПОУ «Красноярский монтажный колледж».

Реализация программы практики предполагает наличие следующего специального помещения:

– лаборатории «Информационной безопасности телекоммуникационных систем».

### 4.2. Информационное обеспечение практики

**Перечень рекомендуемых учебных изданий, дополнительной литературы, Интернет-ресурсов.**

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы, для использования в образовательном процессе.

При формировании библиотечного фонда образовательной организации выбираются не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

#### 4.2.1 Печатные издания

1.Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учрежд. СПО / В.Я. Ищейнов, М.В. Мецатунян. – М.: Форум: ИНФРА–М, 2015. –208с. – ISBN 978–5–00091–079–5.

2.Мельников, Д.А. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.А. Мельников. – 2–е изд., стер. – М.: ФЛИНТА, 2014.–488с. ISBN 978–5–9765–1613–7. Режим доступа: http://znanium.com/ bookread.php?book=402654.

3.Программно-аппаратная защита информации [Электронный ресурс]: Учебное пособие / П.Б. Хорев. – 2–е изд., испр. и доп. – М.: Форум: НИЦ ИНФРА–М, 2015. – 352с. ISBN 978–5–00091–004–7. Режим доступа: http://znanium.com/ bookread.php?book=462645.

4.Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие. – М.: ФОРУМ: ИНФРА–М, 2016. – 520 с. – ISBN 978–5–16–003746–2.

#### 4.2.2. Основные электронные издания

1. Минкомсвязь России [Электронный ресурс]: официальный сайт. – Режим доступа: http://www.minsvyaz.ru/, свободный.

2.Федеральное агентство связи (Россвязь) [Электронный ресурс]: официальный сайт. – Режим доступа: http://www.rossvyaz.ru/, свободный.

3.Comnews. Новости телекоммуникаций, вещания и ИТ [Электронный ресурс]: ежедневная Интернет–газета. – Режим доступа: http://www.comnews.ru/, свободный.

4. Connect! Мир связи [Электронный ресурс]: сетевой журнал. – Режим доступа: http://www.connect.ru/, свободный.

5.CRN: ИТ–бизнес [Электронный ресурс]: сетевое информационное издание. – Режим доступа: http://www.cm.ru/, свободный.

6.Mobile Review [Электронный ресурс]: портал мобильных технологий. – Режим доступа: http://www.mobile–review.com/, свободный.

7.PC–magazine [Электронный ресурс]: сайт журнала. – Режим доступа: http://www.pcmag.ru/, свободный.

8. ГП Телеком [Электронный ресурс]: официальный сайт. – Режим доступа: http://www.gptelecom.ru/, свободный.

9. Библиотека учебных курсов Microsoft [Электронный ресурс]. – Режим доступа: http://msdn.microsoft.com/ru–ru/gg638594, свободный.

10.Интернет–Университет информационных технологий. Библиотека учебных курсов [Электронный ресурс]. – Режим доступа: http://old.intuit.ru, свободный.

11.Компоненты и технологии [Электронный ресурс]: сетевой журнал. – Режим доступа: http://www.kit–e.ru/, свободный.

12.Открытые системы [Электронный ресурс]. – Режим доступа: http://www.osp.ru/, свободный.

13. Сети и системы связи [Электронный ресурс]: архив журнала. – Режим доступа: http://www.ccc.ru/, свободный.

14. Системы управления, связи и безопасности [Электронный ресурс]: сетевой электронный журнал. – Режим доступа: http://sccs.intelgr.coin/, свободный.

15.Современные телекоммуникации России [Электронный ресурс]: отраслевой информационно-аналитический онлайн-журнал. – Режим доступа: http: //www.telecomru.ru/, свободный.

16.Электронная Россия [Электронный ресурс]: информационный сайт. – Режим доступа: http://www.elrussia.ru/, свободный.

17.Электросвязь [Электронный ресурс]: сайт журнала. – Режим доступа: http://www.elsv.ru/, свободный.

18.SecurityLab. Защита информации и информационная безопасность [Электронный ресурс]: информационный портал/ООО "Positive Technologies". – Режим доступа: http://www.securitylab.ru, свободный.

19.Сайт журнала «Специальная техника» [Электронный ресурс]. – Режим доступа: http://ess.ru/ index.htin, свободный.

20.Сайт Федеральной службы безопасности России (ФСБ России) [Электронный ресурс]. – Режим доступа: http://vAvw.fsb.rn, свободный.

21.Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/, свободный.

22.Сайт проекта Общие критерии оценки безопасности информационных технологий [Электронный ресурс]. – Режим доступа: http://www.coinmon criteriaportal.org/, свободный.

**4.2.3. Дополнительные источники**

1.Фороузан, Б.А. Криптография и безопасность сетей: пер. с англ. Под ред. А.Н. Берлина [Электронный ресурс] – М.: Интернет–Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2014. –784 с. Режим доступа: http://znanium.com/bookread.php?book=402618.

2.Информационная безопасность России [Электронный ресурс]. Аналитический сборник: выпуск №1, январь 2016.–128 с. Режим доступа: http://znanium.com/bookread.php?book=402702.

3.Техническая диагностика современных цифровых сетей связи. Основные принципы и технические средства измерений параметров передачи для сетей PDH, SDH, IP, Ethernet и ATM /И.И.Власов, Э.В.Новиков, М.М.Птичников, Д.В.Сладких; под ред. М.М. Птичникова. – М.: Горячая линия–Телеком, 2015. – 580 с. – ISBN 978–5–9912–0195–7.

**4.3. Общие требования к организации практики**

Освоение производится в соответствии с учебным планом по специальности 11.02.15 Инфокоммуникационные сети и системы связи и графиком учебного процесса, утверждённым директором колледжа.

Образовательный процесс организуется строго по расписанию занятий, утвержденному директором колледжа. Учебная практика проводится концентрировано после изучения тем междисциплинарного курса МДК.03.01 Защита информации в

инфокоммуникационных системах и сетях связи.

Текущий учет результатов освоения УП.03 производится в учебном журнале. Наличие оценок по выполнению практических занятий является для каждого студента обязательным.

Практические занятия проводятся в специально оборудованной лаборатории «Информационной безопасности телекоммуникационных систем».

Результатом освоения УП выступают профессиональные компетенции (ПК), оценка которых представляет собой создание и сбор свидетельств деятельности на основе заранее определенных критериев.

С целью оказания помощи студентам при освоении теоретического и практического материала, выполнения самостоятельной работы разрабатываются технологические карты.

Итогом учебной практики УП.03 является дифференцированный зачет. Итоговая оценка выставляется как медиана по результатам выполнения всех заданий.

**4.4. Кадровое обеспечение практики.**

Реализация УП.03обеспечивается педагогическими кадрами, имеющими высшее образование, соответствующее профилю преподаваемого модуля. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального учебного цикла, эти преподаватели получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в профильных организациях не реже раз в три года.

# 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Основным показателем результатов подготовки является освоение профессиональных компетенций:

| **Результаты (освоенные профессиональные компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности | ОПОР 1 – Грамотное классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи.<br>ОПОР 2 – Полный и обоснованный анализ угроз и уязвимостей сетевой безопасности IP–сетей, беспроводных и корпоративных сетей.<br>ОПОР 3 – Грамотное определение возможных сетевых атак и способов несанкционированного доступа в конвергентных системах связи.<br>ОПОР 4 – Умение осуществить мероприятия по проведению аттестационных работ и выявлению каналов утечки.<br>ОПОР 5 – Грамотное выявление недостатков систем защиты в системах и сетях связи с использованием специализированных программных продуктов.<br>ОПОР 6 – Умение тестировать системы с целью определения уровня защищенности, правильность определения уровень защищенности. | **Текущий контроль в форме:**<br>– наблюдения во время выполнения заданий;<br>– защиты практических и лабораторных работ;<br>– проведения анализа по практической работе;<br>– написания рефератов;<br>– тестирования;<br>– экспертное наблюдение за выполнением различных видов работ во время учебной/ производственной практик<br>**Промежуточный контроль:**<br>Диф. зачет по МДК (ПМ.03)<br>Экзамен квалификационный по профессиональному модулю.<br>**Экспертная** оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на различных этапах производственной практики. |
| ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. | ОПОР 7 – Грамотный выбор оптимальных способов для обеспечения информационной безопасности.<br>ОПОР 8 – Грамотный выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях. | |
| ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием | ОПОР 9 – Полнота определения мероприятий по защите информации на предприятиях связи, их организация, оптимальные и достаточные способы и методы реализации. ОПОР 10 – Полнота разработки политики безопасности сетевых элементов и логических сетей.<br>ОПОР 11 – Правильность расчета и | |

| | | |
|---|---|---|
| специализированного программного обеспечения и оборудования. | установки специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей, выполнение в соответствии с отраслевыми стандартами.<br>ОПОР 12 – Умение устанавливать и настраивать средства защиты операционных систем, инфокоммуникационных систем и сетей связи в соответствии с отраслевыми стандартами.<br>ОПОР 13 – Умение конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности и отраслевыми стандартами.<br>ОПОР 14 – Умение защитить базы данных при помощи специализированных программных продуктов;<br>ОПОР 15 – Умение защитить ресурсы инфокоммуникационных сетей и систем связи криптографическими методами. | |

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

| **Результаты (освоенные общие компетенции)** | **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;<br>– адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. |
| 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 | |
| ОК 03. Планировать и реализовывать собственное профессиональное личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в | – демонстрация ответственности за принятия решения;<br>– обоснованность самоанализа и коррекция результатов собственной работы; | |

| | | |
|---|---|---|
| различных жизненных ситуациях | | |
| 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;<br>– обоснованность анализа работы членов команды подчиненных) | |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста | – грамотность устной и письменной речи,<br>– ясность формулирования и изложения мыслей | |
| ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения | – соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик, | |
| ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях | – эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;<br>- знание и использование ресурсосберегающих технологий в области телекоммуникаций | |
| ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности | - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; | |
| ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках | - эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту; | |

Моор О.И.

Подписано цифровой подписью: Моор О.И.
DN: cn=Моор О.И., o=КГБПОУ "Краснорский монтажный колледж", ou=Зам.дир. по УР, email=kmkmo@mail.ru, c=RU
Дата: 2023.06.02 16:41:17 +07'00'