МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ РОСТОВСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

РОСТОВСКОЙ ОБЛАСТИ

**«РОСТОВСКИЙ-НА-ДОНУ КОЛЛЕДЖ СВЯЗИ И ИНФОРМАТИКИ»**

РАБОЧАЯ ПРОГРАММА

учебной дисциплины

**ОП.01 «Основы информационной безопасности»**

программы подготовки специалистов среднего звена

для специальности

**10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**

(базовая подготовка)

г. Ростов-на-Дону

2022г.

|  |  |
| --- | --- |
| **ОДОБРЕНО**  На заседании цикловой комиссии  «Информационная безопасность»  Протокол № 1 от 31 августа 2022 года  Председатель ЦК ИБ  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Копылова О.В. | **УТВЕРЖДАЮ:**  Зам. директора по НМР  \_\_\_\_\_\_\_\_\_\_ Подцатова И.В.  «31» августа 2022 года. |

Рабочая программа частично вариативной учебной дисциплины ОП.01 «Основы информационной безопасности» разработана в соответствии с требованиями регионального рынка труда на основании утвержденных на цикловых комиссиях колледжа перечнем знаний, умений и практического опыта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации № 1553 от 9 декабря 2016г., зарегистрированного Министерством юстиции (рег. № 44938 от 26 декабря 2016 г).

Частично вариативная дисциплина ОП.01 «Основы информационной безопасности» профессиональной деятельности по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» утверждена на метод совете протокол № 1 от 31 августа 2022 г. Перечень знаний, умений и практического опыта с учетом потребностей работодателей и особенностей региона, науки и технологии утвержден на заседании цикловой комиссии протокол, в рамках, установленных ФГОС.

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж связи и информатики»

Разработчики:

ОП.01 Основы информационной безопасности, Перевышина Е.А. – преподаватель ГБПОУ РО «РКСИ»

Рецензенты:

Комова О.В. – зам директора по УР ГБПОУ РО «РКСИ»

Масютин А.Н. – Начальник управления системных проектов Ростовского НТЦ ФГУП «НПП «Гамма»

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ………...........................4

[2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 6](#_Toc473204975)

[3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ 9](#_Toc473204980)

[4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ 11](#_Toc473204991)

**1**. **ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**ОП.01 «Основы информационной безопасности**

* 1. **Область применения программы**

Рабочая программа частично вариативной учебной дисциплины ОП.01 «Основы информационной безопасности» является частью программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (базовой подготовки), разработана на основе ФГОС СПО. Частично вариативная дисциплина ОП.01 «Основы информационной безопасности» профессиональной деятельности по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» утверждена на метод совете протокол № 1 от 31 августа 2022 г. Перечень знаний, умений и практического опыта с учетом потребностей работодателей и особенностей региона, науки и технологии утвержден на заседании цикловой комиссии протокол, в рамках, установленных ФГОС.

Рабочая программа предназначена для студентов очной формы обучения.

**1.2 Место учебной дисциплины в структуре образовательной программы**

Учебная дисциплина ОП.01 «Основы информационной безопасности» является общепрофессиональному циклу, является частично вариативной дисциплиной.

**1.3 Цели и задачи дисциплины – требования к результатам освоения дисциплины:**

|  |  |  |
| --- | --- | --- |
| Код ПК, ОК | Умения | Знания |
| ОК 03,  ОК 06,  ОК 07,  ОК 09,  ПК 2.4, | * классифицировать защищаемую информацию по видам тайны и степеням секретности; * классифицировать основные угрозы безопасности информации | * сущность и понятие информационной безопасности, характеристику ее составляющих; * место информационной безопасности в системе национальной безопасности страны; * виды, источники и носители защищаемой информации; * источники угроз безопасности информации и меры по их предотвращению; * факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; * жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; * современные средства и способы обеспечения информационной безопасности; * основные методики анализа угроз и рисков информационной безопасности. |

Дисциплина ОП.01 «Основы информационной безопасности» способствует формированию общих компетенций ОК (3, 6) и профессиональных компетенций ПК (2.4) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»:

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа;

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие;

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей;

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях;

ОК 09. Использовать информационные технологии в профессиональной деятельности;

Вариативная часть по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» используется на увеличение объема времени на изучение тем и выполнение практический занятий в соответствии с потребностями работодателей и спецификой деятельности колледжа, что создает реальные возможности для углубления и расширения умений и знаний будущих специалистов.

Из вариативной части на учебную дисциплину ОП.01 01 «Основы информационной безопасности» отведено **24** часа:

| **Наименование темы** | **Кол-во часов** | **Дополнительные умения** | **Дополнительные знания** | **Формируемые компетенции** |
| --- | --- | --- | --- | --- |
| 1.3 Угрозы безопасности защищаемой информации | 4 | классифицировать нарушителейприменять различные методы шифрования, методом подстановкиклассифицировать вирусы; алгоритмы шифрования различными методами | типы нарушителей  * различные технические средства, такие как электронные уши, средства перехвата телефонной связи, средства скрытого наблюдения и поиска, средства контроля компьютеров и сетей, средства приема, записи и управления * сущность функционирования программных закладок  основные возможности антивирусов | ОК 01  ОК 04  ПК 2.2. |
| 1.4 Средства используемые злоумышленником | 4 |
| 2.3 Защита информации в автоматизированных (информационных) системах | 4 |
| Самостоятельная работа. | 2 |
| Консультации | 2 |
| Экзамен | 8 |
| **Всего** | **26** | **-** | **-** | **-** |

1.4 Практическая подготовка при реализации учебных дисциплин путем проведения практических и лабораторных занятий занимает 2**0 часов**.

| **Наименование темы** | **Наименование тем практических работ в форме практической подготовки с учетом специфики осваиваемой специальности** | **Количество часов** |
| --- | --- | --- |
| Тема 1.1 Основные понятия и задачи информационной безопасности | Практическое занятие №1 Доктрина ИБ РФ. | 2 |
| Тема 1.2 Основы защиты информации | Практическое занятие №2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности. | 2 |
| Практическое занятие №3. Виды информации ограниченного доступа | 2 |
| Тема 1.3 Угрозы безопасности защищаемой информации | Практическое занятие №4. Описание объекта защиты | 2 |
| Практическое занятие №5. Определение угроз объекта информатизации и их классификация | 2 |
| Тема 2.1 Методологические подходы к защите информации | Практическое занятие №6. Выбор мер защиты информации для автоматизированного рабочего места | 2 |
| Тема 2.2 Нормативно правовое регулирование защиты информации | Практическое занятие №7. Основные положения закона ФЗ 149 | 2 |
| Практическая работа №8. Лицензирование деятельности и сертификация средств в области ЗИ конфиденциальной информации | 2 |
| Тема 2.3 Защита информации в автоматизированных (информационных) системах | Практическое занятие №9. Создание системы информационной безопасности предприятия | 2 |
| Практическое занятие №10. Обеспечение защиты информации при работе с кадрами | 2 |

***В рамках программы у обучающихся формируются личностные результаты:***

|  |  |
| --- | --- |
| **Личностные результаты**  **реализации программы воспитания**  *(дескрипторы)* | **Код личностных результатов  реализации  программы  воспитания** |
| Осознающий себя гражданином и защитником великой страны | **ЛР 1** |
| Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций | **ЛР 2** |
| Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих | **ЛР 3** |
| Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа» | **ЛР 4** |
| Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности. | **ЛР 7** |
| Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой | **ЛР 10** |
| Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания | **ЛР 12** |
| Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности | **ЛР 13** |
| Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности | **ЛР 14** |
| Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем | **ЛР 15** |
| Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению | **ЛР16** |
| Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение | **ЛР17** |

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

**2.1. Объем учебной дисциплины и виды учебной работы**

|  |  |
| --- | --- |
| **Вид учебной работы** | ***Объем часов*** |
| **Объём ОП (всего)** | ***74*** |
| **Обязательная аудиторная учебная нагрузка (всего)** | ***62*** |
| в том числе: |  |
| теоретическое обучение | *42* |
| практические занятия | *20* |
| Консультации | ***4*** |
| Вариативная часть | ***26*** |
| *Промежуточная аттестация* | ***8*** |
| *Итоговая аттестация - экзамен* |  |

# **2.2. Тематический план и содержание учебной дисциплины**

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование разделов и тем** | **Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект)**  *(если предусмотрены)* | **Объем часов** | **Осваиваемые элементы компетенций** |
| **1** | **2** | **3** | **4** |
| **Раздел 1 Теоретические основы информационной безопасности** | | ***36*** |  |
| **Тема 1.1**  Основные понятия и задачи информационной безопасности | **Содержание учебного материала** | ***4*** |  |
| Сущность и понятие информационной безопасности. | 2 | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ОК 3, ОК 6, ОК 9, ПК.2.4 |
| Сущность функционирования системы защиты информации. | 2 |
| **Практические работы** | **2** |
| Практическое занятие №1 Доктрина ИБ РФ. | 2 |
| **Тема 1.2**  Основы защиты информации | **Содержание учебного материала** | ***8*** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ОК 3, ОК 6, ОК 9, ПК.2.4 |
| Государственная тайна | *2* |
| Конфиденциальная информация | *2* |
| Цели и задачи защиты информации. | *2* |
| Политика безопасности | *2* |
| **Практические работы** | ***4*** |
| Практическое занятие №2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности. | *2* |
| Практическое занятие №3. Виды информации ограниченного доступа | *2* |
| **Тема 1.3**  Угрозы безопасности защищаемой информации | **Содержание учебного материала** | ***8*** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ОК 3, ОК 6, ОК 9, ПК.2.4 |
| Угрозы безопасности информации | *2* |
| Модель нарушителя | *2* |
| Каналы и методы несанкционированного доступа к информации | *2* |
| Уязвимости. Методы оценки уязвимости информации | *2* |
| **Практические работы** | ***4*** |
| Практическое занятие №4. Описание объекта защиты | *2* |
| Практическое занятие №5. Определение угроз объекта информатизации и их классификация | *2* |
| **Тема 1.4**  Средства используемые злоумышленником | **Содержание учебного материала** | ***6*** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ОК 3, ОК 6, ОК 9, ПК.2.4 |
| Технические средства добывания информации | *2* |
| Программные средства добывания информации | *2* |
| Компьютерные вирусы | *2* |
| **Раздел 2 Методология защиты информации** | | ***24*** |  |
| **Тема 2.1**  Методологические подходы к защите информации | **Содержание учебного материала** | ***4*** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ОК 3, ОК 6, ОК 9, ПК.2.4 |
| Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. | *2* |
| Виды мер и основные принципы защиты информации. | *2* |
| **Практические работы** | ***2*** |
| Практическое занятие №6. Выбор мер защиты информации для автоматизированного рабочего места | *2* |
| **Тема 2.2**  Нормативно правовое регулирование защиты информации | **Содержание учебного материала** | ***4*** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ОК 3, ОК 6, ОК 9, ОК 10 |
| Российские и международные стандарты, определяющие требования к защите информации. | *2* |
| Система сертификации РФ в области защиты информации | *2* |
| **Практические работы** | ***4*** |
| Практическое занятие №7. Основные положения закона ФЗ 149 | *2* |
| Практическая работа №8. Лицензирование деятельности и сертификация средств в области ЗИ конфиденциальной информации | *2* |
| **Тема 2.3**  Защита информации в автоматизированных (информационных) системах | **Содержание учебного материала** | ***6*** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ОК 3, ОК 6, ОК 9, ПК.2.4 |
| Криптографическая защита информации | *2* |
| Инженерная защита и техническая охрана объектов информатизации | *2* |
| Организационно-распорядительная защита информации. | *2* |
| **Практические занятия** | ***4*** |
| Практическое занятие №9. Создание системы информационной безопасности предприятия | *2* |
| Практическое занятие №10. Обеспечение защиты информации при работе с кадрами | *2* |
| **Всего:** | | ***74*** |  |

# 

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

**3.1. Требования к минимальному материально-техническому обеспечению**

Для реализации программы учебной дисциплины ОП.01 «Основы информационной безопасности» имеется в наличии:

* технические средства обучения:
* посадочные места по количеству обучаемых;
* рабочее место преподавателя;
* необходимая методическая и справочная литература (в т.ч. в электронном в виде).
* средства информационных технологий (мультимедийный проектор, интерактивная доска, ПК, программное обеспечение):
* персональные компьютеры по количеству обучаемых;
* интерактивный видеопроектор;
* доступ к сети Интернет;
* ОС Windows, Linux;
* браузеры Google Chrome, Mozilla Firefox идр.

**3.2. Информационное обеспечение обучения**

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

**Основные источники:**

1. Внуков Андрей Анатольевич. Основы информационной безопасности: защита информации. Изд-во ЮРАЙТ-Восток 2020
2. Нестеров Сергей Александрович. Основы информационной безопасности. Учебник для СПО. Издательство Лань, 2021
3. Баранова Е.К. Основы информационной безопасности. Учебник. Изд-во Инфра-М, 2019
4. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы

информационной безопасности. –М.: Академия. 2015.

1. Шаньгин В. Ф.. Информационная безопасность и защита информации.   
   ДМК Пресс. 2018.
2. Нестеров С.А. Основы информационной безопасности. – Издательство Лань. 2019.
3. [Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. 201](https://www.ozon.ru/context/detail/id/137707095/)8
4. Гультяева Т.А. Основы информационной безопасности. Новосибирский государственный технический университет. 2018

**Дополнительные источники:**

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ.
2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебн. пособие для вузов. - М: Горячая линия-Телеком, 2018. - 544 с.: ил. Допущено УМО ИБ.
3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2019.
4. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М.: КНОРУС, 2019.
5. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2018.
6. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности. –М.: Академия. 2018.
7. Проскурин В.Г. Защита программ и данных: Учебное пособие для ВУЗов. - –М.: Академия. 2018.
8. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2019.
9. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. ДМК Пресс, 2019.

**Периодические издания:**

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

**Электронные источники:**

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

**Контроль** **и оценка** результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, устных опросов, тестирования, а также выполнения студентами домашних заданий, индивидуальных заданий, и регламентируется локальным Положением о текущем контроле и промежуточной аттестации студентов ГБПОУ РО «РКСИ».

|  |  |  |
| --- | --- | --- |
| **Результаты обучения** | **Критерии оценки** | **Формы и методы**  **контроля и оценки**  **результатов обучения** |
| **ЛР 1**  Осознающий себя гражданином и защитником великой страны  **ЛР 2**  Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций  **ЛР 3**  Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих  **ЛР 4**  Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»  **ЛР 7**  Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.  **ЛР 10**  Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой  **ЛР 12**  Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания  **ЛР 13**  Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности  **ЛР 14**  Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности  **ЛР 15**  Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных  проблем  **ЛР16**  Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению  **ЛР17**  Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение  **ЛР18**  Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве  **ЛР19**  Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей  информации  **ЛР20**  Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели) труда, либо иные схожие характеристики | демонстрация интереса к будущей профессии;  оценка собственного продвижения, личностного развития;  положительная динамика в организации собственной учебной деятельности по результатам самооценки, самоанализа и коррекции ее результатов;  ответственность за результат учебной деятельности и подготовки к профессиональной деятельности;  проявление высокопрофессиональной трудовой активности;  участие в исследовательской и проектной работе;  соблюдение этических норм общения при взаимодействии с обучающимися, преподавателями, мастерами и руководителями практики;  конструктивное взаимодействие в учебном коллективе/бригаде;  готовность к общению и взаимодействию с людьми самого разного статуса, этнической, религиозной принадлежности и в многообразных обстоятельствах;  проявление мировоззренческих установок на готовность молодых людей к работе на благо Отечества;  проявление правовой активности и навыков правомерного поведения, уважения к Закону;  отсутствие фактов проявления идеологии терроризма и экстремизма среди обучающихся;  проявление культуры потребления информации, умений и навыков пользования компьютерной техникой, навыков отбора и критического анализа информации, умения ориентироваться в информационном пространстве;  проявление экономической и финансовой культуры, экономической грамотности, а также собственной адекватной позиции по отношению к социально-экономической действительности. | анализ соблюдения норм и правил поведения, принятых в колледже, обществе, профессиональном сообществе;  анализ самооценки событий обучающимися;  педагогический и психологический мониторинг;  анализ проявления обучающимися качеств своей личности: оценка поступков, осознание своей жизненной позиции, культурного выбора, мотивов личностных целей; анализ портфолио. |
| ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа;  ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие;  ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей;  ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях;  ОК 09. Использовать информационные технологии в профессиональной деятельности; | оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач;  оценка «хорошо» выставляется обучающемуся, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения;  оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач;  оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно. | Контроль знаний и умений осуществляется в ходе выполнения практических и лабораторных работ, промежуточной аттестации.  Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы  Экспертное заключение преподавателя |

Лист согласования

**Дополнения и изменения к рабочей программе на учебный год**

Дополнения и изменения к рабочей программе на \_\_\_\_\_\_\_\_\_\_ учебный год по дисциплине Наименование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В рабочую программу дисциплины «…» внесены следующие изменения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дополнения и изменения в рабочей программе дисциплины «….» обсуждены на заседании ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Протокол № \_\_\_\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_\_г.

Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_