Министерство образования и науки РТ
Государственное автономное профессиональное
образовательное учреждение
«КАЗАНСКИЙ РАДИОМЕХАНИЧЕСКИЙ КОЛЛЕДЖ»

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.15 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

по программе подготовки специалистов среднего звена
по специальности среднего профессионального образования
09.02.01 «Компьютерные системы и комплексы»
(базовой подготовки)

Казань, 2021

Программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования образовательной программы подготовки специалистов среднего звена (далее – СПО ППССЗ) 09.02.01 «Компьютерные системы и комплексы».

Организация-разработчик: ГАПОУ «Казанский радиомеханический колледж»

Разработчик:
Мусина Марина Владимировна, преподаватель
первая квалификационная категория

РАССМОТРЕНО
Предметной цикловой комиссией
Протокол № 1 от « 3 » 09 2021 г.
Председатель ПЦК _____

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения программы

Программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности среднего профессионального образования образовательной программы подготовки специалистов среднего звена (далее – СПО ППССЗ) 09.02.01 «Компьютерные системы и комплексы».

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы

Программа учебной дисциплины «Информационная безопасность» входит в профессиональный цикл «Общепрофессиональные дисциплины».

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины:

В результате освоения учебной дисциплины обучающийся должен

уметь:

- выполнять анализ способов нарушения информационной безопасности;
- использовать методы и средства защиты данных;
- применять алгоритмы криптографии;
- пользоваться средствами защиты, предоставляемыми СУБД;
- создавать дополнительные средства защиты;
- проводить анализ и оценивание механизмов защиты;
- выбирать формы и критерии информационной безопасности;
- разрабатывать предложения по совершенствованию политики безопасности;

знать:

- терминологию в сфере безопасности информационного контента;
- понятия политики безопасности, существующие типы политик безопасности;
- существующие стандарты информационной безопасности;
- виды угроз информационной безопасности;
- средства борьбы с угрозами информационной безопасности;
- о современных концепциях безопасности программного обеспечения и баз данных;
- методы защиты информации;
- критерии защищенности программного обеспечения и баз данных;
- угрозы безопасности программного обеспечения и баз данных;
- критерии и методы оценивание механизмов защиты;
- организационно-правовое обеспечение информационной безопасности.

Результаты освоения дисциплины направлены на формирование общих и профессиональных компетенций (ОК/ПК), результатов воспитания:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ПК 1.2. Разрабатывать схемы цифровых устройств на основе интегральных схем разной степени интеграции.
ПК 1.5. Выполнять требования нормативно-технической документации.
ПК 3.1. Проводить контроль параметров, диагностику и восстановление работоспособности компьютерных систем и комплексов.
ЛР6 Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации.
ЛР13 Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации.
ЛР14 Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм.
ЛР17 Обладающий навыками креативного мышления, применения нестандартных методов в решении производственных проблем.
ЛР18 Осознанно выполняющий профессиональные требования, добросовестный, способный четко организовывать и планировать свою трудовую деятельность, нацеленный на результат.

1.4. Количество часов на освоение программы учебной дисциплины

Максимальная учебная нагрузка обучающегося 144 часа, в том числе:
- обязательная аудиторная учебная нагрузка обучающегося 96 часов;
- самостоятельная работа обучающегося 48 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	*Объем часов*
Максимальная учебная нагрузка (всего)	144
Обязательная аудиторная учебная нагрузка (всего)	96
в том числе:	
теоретические занятия	40
практические занятия	56
лабораторные занятия	
в форме практической подготовки	56
курсовой проект (работа)	
Самостоятельная работа обучающегося (всего)	48
Итоговая аттестация в форме ***комплексного дифференцированного зачета***	

2.2. Тематический план и содержание учебной дисциплины ОП.15 Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа обучающихся		Объем часов	Уровень освоения
1	2		3	4
Раздел 1. Информация как объект защиты				
Тема 1.1. Основные виды информационной защиты. Защита человека как собственника информации.	**Содержание учебного материала**		**1**	
	1.	Понятие об опасной информации. Виды опасной информации. Способы защиты человека от излишней, назойливой, недобросовестной информации. Вредная информация в формах обмана и злоупотребления доверием. Ценность информации	1	2
	Самостоятельная работа Формирование прав собственности на информацию		4	
Тема 1.2 Уровни представления информации и особенности ее защиты.	**Содержание учебного материала**		**1**	
	1.	Виды и общая характеристика информационных угроз. Уязвимости информационных систем. Виды ущерба от информационных атак. Носители информационных угроз.	1	2
Тема 1.3 Классификация и категории информационных нарушителей.	**Содержание учебного материала**		**2**	
	1.	Информационные нарушители. Цели нарушителей. Оценка опасности нарушителя на основании его осведомленности, оснащенности и подготовленности. Ресурсы нарушителя. Оценка рисков неправомерного доступа для объекта атаки и нарушителя. Сложившиеся приоритеты в выборе тактики действий нарушителя	2	2
	Практические занятия **(практическая подготовка)**		**10**	
	1	Оценка агентов угроз и угроз	2	3
	2	Разработка классификации агентов угроз	2	3
	3	Упорядочивание угроз и механизмов угроз в соответствии с классификацией агентов угроз	2	3
	4	Оценка вероятности угроз, инициируемых преднамеренными агентами	2	3
	5	Оценка уязвимости	2	3
	Самостоятельная работа Создание перечня информационного контента, агентов угроз и угроз на индивидуальном предприятии. Выполнение анализа угроз и уязвимости		4	

Раздел 2. Направления информационной защиты				
Тема 2.1 Нормативно-правовое регулирование защиты информации.	**Содержание учебного материала**		**2**	
	1.	Характеристика нормативно-правовой защиты. Виды информации по категории доступа. Правовой режим защиты государственной тайны. Правовой режим защиты конфиденциальной информации. Виды конфиденциальной информации и режимы ее защиты. Ответственность за право нарушения в сфере защиты конфиденциальной информации	2	2
	Самостоятельная работа Используя Интернет – ресурсы ознакомиться со статьями 23,24 Конституции РФ, статьями 272, 273, 274, 138, 146, 283, 284 главы 28 Уголовного кодекса РФ.		4	
Тема 2.2 Организационно-распорядительная защита	**Содержание учебного материала**		**2**	
	1.	Работа с кадрами и внутри объектовый режим. Основные принципы организационнораспорядительной защиты: изоляция носителей информации, минимальная информированность исполнителей, производственная дисциплина, регламентация служебного времени, минимизация неслужебных контактов, объединение и разделение полномочий. Формы контроля и надзора за персоналом. Дезинформация и легендирование. Допуск к работе с конфиденциальной информацией. Режим учета и хранения вещественных носителей информации. Права и обязанности системного администратора. Функции подразделений безопасности	2	2
	Самостоятельная работа Используя Интернет – ресурсы ознакомиться Кодексом РФ об административных нарушениях № 195-ФЗ от 30.12.2001 (с изм. и доп. от 4.07.2003), Гражданским кодексом РФ. Часть четвертая, ФЗ «О персональных данных», № 152-ФЗ от 27.07.2006, ФЗ «Об информации, информационных технологиях и защите информации», № 149-ФЗ от 27.07.2006		4	
Тема 2.3 Инженерно-техническая защита от физического вторжения.	**Содержание учебного материала**		**2**	
	1.	Защита информации от утечки по техническим каналам. Защита от внедрения и использования автономных средств технической разведки. Управление доступом к информации. Защита компьютерных систем от вредоносного программного воздействия. Семантическое скрытие информации. Обеспечение нормальных условий эксплуатации информационных систем и машинных носителей	2	2

		информации		
	Практические занятия **(практическая подготовка)**		**16**	
	1	Определение шагов для формального анализа риска.	4	3
	2	Определение активов для включения в список при анализе риска.	4	3
	3	Разработка качественных шкал для оценки активов.	4	3
	4	Определение значений суммарного влияния для качественного анализа риска.	4	3
	Самостоятельная работа Создание перечня подразделений безопасности на индивидуальном предприятии. Создание перечня организационно-распорядительных и инженерно-технических мероприятий на индивидуальном предприятии		4	
Раздел 3. Методы и средства защиты программного обеспечения				
Тема 3.1. Описание типовых политик безопасности	**Содержание учебного материала**		**2**	
	1.	Понятие политики безопасности. Модель политики безопасности.	2	2
	Практические занятия **(практическая подготовка)**		**4**	
	1	Оценка политик безопасности	4	3
Тема 3.2. Модель защищенного канала связи	**Содержание учебного материала**		**2**	
	1	Виды информационных угроз для канала связи и передаваемой информации. Незаконное использование канала. Деструктивные действия. Фальсификация передаваемых данных. Подключение к каналу связи своих передатчиков и приемников. Виды перехвата информации в канале связи. Использование побочных каналов утечки информации. Способы защиты передаваемой информации от характерных атак	2	2
	Самостоятельная работа Технические характеристики устройств (передатчиков и приемников), подключаемых к каналу связи		4	
Тема 3.3. Основные принципы создания программноаппаратных средств обеспечения информационной	**Содержание учебного материала**		**2**	
	1	Концепция диспетчера доступа. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите. Их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем	2	2

безопасности.				
Тема 3.4. Угрозы безопасности компьютерных систем	**Содержание учебного материала**		**2**	
	1	Методы и средства ограничения доступа к компонентам вычислительных систем. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства хранения ключевой информации.	2	2
	Самостоятельная работа Создание перечня методов и средств защиты ПО на индивидуальном предприятии		4	
Тема 3.5. Защита программ	**Содержание учебного материала**		**2**	
	1	Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности.	2	3
Раздел 4. Механизмы обеспечения информационной безопасности программного обеспечения и баз данных				
Тема 4.1. Анализ существующих средств и методов защиты программного обеспечения	**Содержание учебного материала**		**2**	
	1	Классификация системы защиты программного обеспечения по методу установки, по используемым механизмам защиты. Методы для защиты ПО: Алгоритмы запутывания, Алгоритмы мутации, Алгоритмы компрессии данных, Алгоритмы шифрования данных, Вычисление сложных математических выражений в процессе отработки механизма защиты, Методы затруднения дизассемблирования, Нестандартные методы работы с аппаратным обеспечением. Классификация системы защиты по принципу функционирования системы защиты. Достоинства и недостатки методов.	2	3
	Практические занятия **(практическая подготовка)**		**8**	
	1	Создание системы защиты ПО, применяя к программному обеспечению алгоритмы мутации	4	2
	2	Создание системы защиты ПО, применяя к программному обеспечению методы затруднения дизассемблирования.	4	2
	Самостоятельная работа Методы затруднения отладки, Эмуляция процессоров и операционных систем. Достоинства и недостатки методов.		4	
Тема 4.2. Классификация угроз конфиденциальности	**Содержание учебного материала**		**2**	
	1	Причины, виды, основные методы нарушения конфиденциальности. Типы утечки	2	2

СУБД.		конфиденциальной информации из СУБД, частичное разглашение. Соотношение защищенности и доступности данных. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов.		
Тема 4.3. Методы противодействия.	**Содержание учебного материала**		**2**	
	1	Особенности применения криптографических методов. Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД.	2	2
	Практические занятия **(практическая подготовка)**		**8**	
	1.	Создание системы защиты ПО, применяя криптографические методы.	4	3
	2.	Модификация системы, разделяя группы пользователей, привилегии, роли и представления информации	4	3
	Самостоятельная работа Этапы развития криптографии. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа.		4	
Тема 4.4. Метки безопасности	**Содержание учебного материала**		**1**	
	1.	Использование представлений для обеспечения конфиденциальности информации в СУБД	1	2
	Самостоятельная работа Произвести сравнительный анализ достоинств и недостатков изученных ранее СУБД		4	
Тема 4.5. Аудит и подотчетность	**Содержание учебного материала**		**1**	
	1.	Подотчетность действий пользователя и аудит связанных с безопасностью событий. Журнализация. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации	1	2
Тема 4.6. Оценка эффективности систем защиты	**Содержание учебного материала**		**2**	2
	1.	Набор показателей применимости и критериев оценки систем защиты программного обеспечения. Показатели применимости: Технические, Экономические,	2	2

		Организационные. Критерии оценки: Защита как таковая, Стойкость к исследованию/взлому, Отказоустойчивость (надёжность), Независимость от конкретных реализаций ОС, Совместимость, Неудобства для конечного пользователя ПО, Побочные эффекты, Стоимость, Доброкачественность		
	Практические занятия **(практическая подготовка)**		**4**	
	1	Произвести технический, экономический и организационный анализ показателей применимости программного обеспечения отраслевой направленности Произвести оценку критериев системы защиты программного обеспечения отраслевой направленности.	4	3
Раздел 5. Обеспечение информационной безопасности компьютерных сетей				
Тема 5.1. Программно-аппаратные средства защиты информации в сетях передачи данных.	**Содержание учебного материала**		**2**	
	1	Модели безопасного взаимодействия в КС. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды.	2	2
Тема 5.2. Межсетевые экраны.	**Содержание учебного материала**		**2**	
	1	Свойства экранирующего субъекта. Классификация требований к классам межсетевых экранов	2	2
	Практические занятия **(практическая подготовка)**		**4**	
	1	Создание модели политики безопасности индивидуального предприятия на основе собранных данных	4	3
	Самостоятельная работа Создание перечня систем идентификации и аутентификации на индивидуальном предприятии. Аудит журналов брандмауэра.		4	
Раздел 6. Организационно-правовое обеспечение информационной безопасности				
Тема 6.1. Правовое обеспечение информационной безопасности.	**Содержание учебного материала**		**2**	
	1.	Правовое обеспечение информационной безопасности. Российские документы по защите информации. Организационное обеспечение информационной безопасности	2	2
Тема 6.2. Состав и назначение должностной инструкции.	**Содержание учебного материала**		**2**	
	1.	Состав и назначение должностной инструкции.	2	2
	Практические занятия **(практическая подготовка)**		**2**	

	1.	Составление должностной инструкции	2	2
	Самостоятельная работа Методы контроля за исполнением должностных инструкций. Методы и формы организационной защиты информации. Методы организационной защиты информации. Виды перекрытия каналов утечки информации		4	
Дифференциальный зачёт			**2**	
		Всего:	**156**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия учебного кабинета «Компьютерный кабинет».
Оборудование учебного кабинета:
- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-наглядных пособий.

Технические средства:
- компьютер с лицензионным программным обеспечением;
- современные ПК, объединённые в локальную сеть;
- мультимедиа проектор;
- экран.

Оборудование кабинета:
- рабочее место преподавателя;
- посадочные места по количеству обучающихся;
- персональные компьютеры с установленным ПО.

Технические и программные средства обучения:
- выход в ЛВС с каждого ПК на студенческий сервер;
- ПК с установленным ПО: ОС Windows, СУБД MS Access 2010, MS Visio 2010;
- комплект учебно-методической документации на студенческом сервере.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. — М.: ИД «ФОРУМ»: ИНФРА-М, 2017. — 416 с. — (Профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/775200

2. Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф. Шаньгин. — М.: ИД «ФОРУМ»: ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/546679 II

Дополнительные источники:

1. Андрианова Т.В. СУБД MS Access 2010. Электронное учебное пособие. – Н. Новгород, АНПОО «НКТС», 2016.– 63 с.

2. Андрианова Т.В. СУБД MS Access 2010. Лабораторный практикум. Электронное пособие. – Н. Новгород, АНПОО «НКТС», 2016.– 42 с.

Интернет-ресурсы:

ZNANIUM.COM [ЭБС]
http://znanium.com/
http://biblioclub.ru
https://biblio-online.ru/
https://www.book.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения: - выполнять анализ способов нарушения информационной безопасности; - использовать методы и средства защиты данных; - применять алгоритмы криптографии; - пользоваться средствами защиты, предоставляемыми СУБД; - создавать дополнительные средства защиты; - проводить анализ и оценивание механизмов защиты; - выбирать формы и критерии информационной безопасности; - разрабатывать предложения по совершенствованию политики безопасности; **Знания**: - терминологию в сфере безопасности информационного контента; - понятия политики безопасности, существующие типы политик безопасности; - существующие стандарты информационной безопасности; - виды угроз информационной безопасности; - средства борьбы с угрозами информационной безопасности; - о современных концепциях безопасности программного обеспечения и баз данных; - методы защиты информации; - критерии защищенности программного обеспечения и баз данных; - угрозы безопасности программного обеспечения и баз данных; - критерии и методы оценивание механизмов защиты; - организационно-правовое обеспечение информационной безопасности.	- Наблюдение за выполнением и оценка результатов практических работ; - Оценка программированного задания. - Устный опрос - Контрольное тестирование - Дифференцированный зачет

с

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 1.2. Разрабатывать схемы цифровых устройств на основе интегральных схем разной степени интеграции.	– демонстрация точности и скорости чтения чертежей; – демонстрация навыков знания требований нормативно-технической документации ГОСТ; – демонстрация навыков и скорости проведения необходимых расчетов; – демонстрация навыков оформления документации на ПК; – демонстрация навыков и скорости работы в среде специализированного программного обеспечения;	Оценка в рамках текущего и промежуточного контроля: - результатов работы на практических занятиях; - результатов выполнения индивидуальной самостоятельной работы; - результатов тестирования. Экспертная оценка результатов деятельности обучающегося при выполнении самостоятельных работ, ответов на контрольные вопросы, тестирования.
ПК 1.5. Выполнять требования нормативно-технической документации.	– демонстрация навыков знания требований нормативно-технической документации ГОСТ; – демонстрация скорости и навыков работы со справочной литературой; – демонстрация скорости принятия и обоснования технических решений; – демонстрация скорости и навыков работы со справочной литературой; – демонстрация навыков и скорости проведения необходимых расчетов;	Оценка в рамках текущего и промежуточного контроля: - результатов работы на практических занятиях; - результатов выполнения индивидуальной самостоятельной работы; - результатов тестирования. Экспертная оценка результатов деятельности обучающегося при выполнении самостоятельных работ, ответов на контрольные вопросы, тестирования.
ПК 3.1. Проводить контроль параметров, диагностику и восстановление работоспособности компьютерных систем и	– соответствие выбранных методов проведения контроля и диагностики работоспособности компьютерных систем и комплексов универсальному алгоритму поиска и устранения неисправностей.	Оценка в рамках текущего и промежуточного контроля: - результатов работы на практических занятиях;

комплексов.	– обоснованность выбора сервисной аппаратуры для контроля и диагностики компьютерных систем и комплексов. – обоснованность применения основных диагностических тестовых программ при проведении диагностики компьютерных систем. – составление и применение алгоритмов для поиска и устранения неисправностей. – результативность выполнения работ по восстановлению работоспособности компьютерных систем и комплексов в соответствии с алгоритмом поиска и устранения неисправностей.	- результатов выполнения индивидуальной самостоятельной работы; - результатов тестирования. Экспертная оценка результатов деятельности обучающегося при выполнении самостоятельных работ, ответов на контрольные вопросы, тестирования.

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

Результаты (освоенные общих компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	– демонстрация интереса к избранной профессии; – участие в групповых, колледжных, городских и краевых конкурсах профессионального мастерства; – активность, инициативность в процессе освоения профессиональной деятельности. – участие в работе научного общества.	Текущий контроль в форме устного опроса по теме, подготовки сообщений, ответов на контрольные вопросы. Экспертная оценка результатов деятельности обучающегося при выполнении домашних работ, тестирования.
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	Правильный выбор способов решения профессиональных задач. Рациональная организация собственной деятельности во время выполнения лабораторных и практических работ	Текущий контроль в форме устного опроса по теме, подготовки сообщений, ответов на контрольные вопросы. Экспертная оценка результатов деятельности обучающегося при выполнении домашних работ, тестирования.
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	– Точность, быстрота и адекватность в стандартных и нестандартных ситуациях, а так же понимание ответственности за выполненные действия	Текущий контроль в форме устного опроса по теме, подготовки сообщений, ответов на контрольные вопросы. Экспертная оценка результатов деятельности обучающегося

		при выполнении домашних работ, тестирования.
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	- Быстрота и точность поиска, обоснованность выбора оптимальность и научность необходимой информации и применения современных технологий ее обработки	Текущий контроль в форме устного опроса по теме, подготовки сообщений, ответов на контрольные вопросы. Экспертная оценка результатов деятельности обучающегося при выполнении домашних работ, тестирования.
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	Рациональность и корректность использования информационных ресурсов в профессиональной и учебной деятельности	Текущий контроль в форме устного опроса по теме, подготовки сообщений, ответов на контрольные вопросы. Экспертная оценка результатов деятельности обучающегося при выполнении домашних работ, тестирования.
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	Адекватность взаимодействия с обучающимися, преподавателями	Текущий контроль в форме устного опроса по теме, подготовки сообщений, ответов на контрольные вопросы. Экспертная оценка результатов деятельности обучающегося при выполнении домашних работ, тестирования.
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	Способность проявлять ответственность за работу членов команды, результат выполнения задания	Текущий контроль в форме устного опроса по теме, подготовки сообщений, ответов на контрольные вопросы. Экспертная оценка результатов деятельности обучающегося при выполнении домашних работ, тестирования.
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	Способность организовывать самостоятельную работу при освоении профессиональных компетенций, проявление стремлений к самообразованию и повышению профессионального уровня	Текущий контроль в форме устного опроса по теме, подготовки сообщений, ответов на контрольные вопросы. Экспертная оценка результатов деятельности обучающегося при выполнении домашних работ, тестирования.
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Готовность быстро и самостоятельно принимать решения в условиях частой смены технологий в профессиональной деятельности.	Текущий контроль в форме устного опроса по теме, подготовки сообщений, ответов на контрольные вопросы. Экспертная оценка результатов деятельности обучающегося при выполнении домашних работ, тестирования.

Результаты **(личностные результаты)**	**Формы и методы контроля и** **оценки результатов воспитания**
ЛР6 Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации.	Оценка наблюдения Оценка тестирования Оценка устного опроса
ЛР13 Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации.	Оценка наблюдения Оценка тестирования Оценка устного опроса
ЛР14 Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм.	Оценка наблюдения Оценка тестирования Оценка устного опроса
ЛР17 Обладающий навыками креативного мышления, применения нестандартных методов в решении производственных проблем.	Оценка наблюдения Оценка тестирования Оценка устного опроса
ЛР18 Осознанно выполняющий профессиональные требования, добросовестный, способный четко организовывать и планировать свою трудовую деятельность, нацеленный на результат.	Оценка наблюдения Оценка тестирования Оценка устного опроса