Автономная некоммерческая профессиональная образовательная организация

«УРАЛЬСКИЙ ПРОМЫШЛЕННО-ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»

**рабочая программа**

учебной дисциплины

**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Специальность:** Программирование в компьютерных системах

2017

|  |  |
| --- | --- |
| Одобрена цикловой комиссией  информатики и вычислительной техники  Председатель комиссии  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ О. Г. Максимова  Протокол №  от « » \_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_г. | Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования, входящей в состав укрупненной группы специальностей «Информатика и вычислительная техника» «Программирование в компьютерных системах»  *УТВЕРЖДАЮ*  Заместитель директора по  учебной работе АН ПОО «Уральский промышленно-экономический техникум»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н.Б. Чмель  « » \_\_\_\_\_\_\_\_\_\_\_\_ 201 \_\_ г. |

Разработчик: **Максимова О.Г.** преподаватель дисциплины

«*Основы информационной безопасности*» АН ПОО «Уральский промышленно-экономический техникум»

Техническая экспертиза рабочей программы

учебной дисциплины «*Основы информационной безопасности»*пройдена.

Эксперты:

Методист АН ПОО «Уральский промышленно-экономический техникум»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Т.Ю. Иванова

Рабочая программа учебной дисциплины содержит следующие разделы:

* паспорт рабочей программы учебной дисциплины;
* структура и содержание учебной дисциплины;
* условия реализации рабочей программы учебной дисциплины;
* контроль и оценка результатов освоения учебной дисциплины

**СОДЕРЖАНИЕ**

[1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 4](#_Toc390283416)

[2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 7](#_Toc390283417)

[3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ 15](#_Toc390283418)

[4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ 17](#_Toc390283419)

# 1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**1.1. Область применения программы**

Программа учебной дисциплины является вариативной частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности среднего профессионального образования 09.02.03 «Программирование в компьютерных системах», входящей в состав укрупненной группы специальностей «Информатика и вычислительная» техника.

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании (в программах повышении квалификации и переподготовки).

**1.2. Место дисциплины в структуре основной профессиональной образовательной программы:**

Дисциплина входит в общепрофессиональный цикл вариативной части.

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

Основной целью изучения дисциплины является формирование знаний об объектах и задачах защиты компьютерных систем, способах и средствах нарушения информационной безопасности, о принципах и подходах к решению задач защиты информации; а также формирование умений по применению современных технологий, выбора средств и инструментов защиты информации для построения современных защищенных информационных систем в соответствии с действующим законодательством.

В результате освоения учебной дисциплины обучающийся должен уметь:

* выбирать средства обеспечения информационной безопасности информационной системы современного предприятия;
* ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему;
* организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа;
* организовывать безопасную работу в Интернет и отправку почтовых сообщений в глобальной сети;
* использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов;
* проводить базовые работы по профилактике нарушений информационной безопасности и построению защищенных информационных систем с использованием стандартных аппаратно­-программных решений.

В результате освоения учебной дисциплины обучающийся должен знать:

* вопросы административного и нормативно-правового обеспечения защиты информации
* основные системы защиты информации в России и в ведущих зарубежных странах;
* основные программно-аппаратные средства и методы защиты информации в компьютерных системах

Содержание дисциплины должно быть ориентировано на подготовку обучающихся по базовой и углубленной подготовке к освоению профессиональных модулей ОПОП по специальности «Программирование в компьютерных системах» и овладению профессиональными компетенциями (ПК):

1. Разработка программных модулей программного обеспечения для компьютерных систем.

ПК 1.1. Выполнять разработку спецификаций отдельных компонент.

ПК 1.2. Осуществлять разработку кода программного продукта на основе готовых спецификаций на уровне модуля.

ПК 1.3. Выполнять отладку программных модулей с использованием специализированных программных средств.

ПК 1.4. Выполнять тестирование программных модулей.

ПК 1.5. Осуществлять оптимизацию программного кода модуля.

ПК 1.6. Разрабатывать компоненты проектной и технической документации с использованием графических языков спецификаций.

2. Разработка и администрирование баз данных.

ПК 2.1. Разрабатывать объекты базы данных.

ПК 2.2. Реализовывать базу данных в конкретной системе управления базами данных (далее - СУБД).

ПК 2.3. Решать вопросы администрирования базы данных.

ПК 2.4. Реализовывать методы и технологии защиты информации в базах данных.

3. Участие в интеграции программных модулей.

ПК 3.1. Анализировать проектную и техническую документацию на уровне взаимодействия компонент программного обеспечения.

ПК 3.2. Выполнять интеграцию модулей в программную систему.

ПК 3.3. Выполнять отладку программного продукта с использованием специализированных программных средств.

ПК 3.4. Осуществлять разработку тестовых наборов и тестовых сценариев.

ПК 3.5. Производить инспектирование компонент программного продукта на предмет соответствия стандартам кодирования.

ПК 3.6. Разрабатывать технологическую документацию.

В результате освоения дисциплины у обучающихся по базовой подготовке формируются общие компетенции (ОК):

* 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 в команде, эффективно общаться с коллегами, руководством, потребителями.
* ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за 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.

**1.4. Рекомендуемое количество часов на освоение программы дисциплины:**

максимальной учебной нагрузки обучающегося120 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 80 часов;

самостоятельной работы обучающегося 40 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)** | **120** |
| **Обязательная аудиторная учебная нагрузка (всего)** | **80** |
| в том числе: |  |
| практические занятия | 20 |
| **Самостоятельная работа обучающегося (всего)** | **40** |
| в том числе: |  |
| анализ информации | 8 |
| анализ защищенности объекта защиты информации | 10 |
| разработка контролирующего, диагностического, демонстрационного материала | 4 |
| составление перечня понятий и определений | 4 |
| подготовка к лабораторным и практическим работам, оформление отчётов | 14 |
| **Итоговая аттестация в форме:**  экзамен | |

2.2. Тематический план и содержание учебной дисциплины «Основы информационной безопасности»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование разделов и тем | Содержание учебного материала, практические занятия,  самостоятельная работа обучающихся | | Объем часов | Уровень освоения |
| 1 | 2 | | 3 | 4 |
| **Раздел 1. Комплексный подход к обеспечению информационной безопасности** | | | **32** |  |
| Тема 1.1  Понятие и составляющие информационной безопасности | Содержание учебного материала | | 4 |
| 1 | Введение в проблему информационной безопасности, ее актуальность. | 1 |
| 2 | Основные объекты информационных систем, подлежащих защите. Цели и задачи обеспечения информационной безопасности для различных объектов (правоохранительные органы, медучреждения, коммерческие организации и др.). | 2 |
| 3 | Основные понятия информационной безопасности. |
| 4 | Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность. |
| 5 | Комплексный подход к защите информации. Уровни формирования режима информационной безопасности: законодательный, административный, процедурный и программно-технический. |
| 6 | Требования к комплексным системам защиты информации. |
| Самостоятельная работа обучающихся | | 4 |  |
| 1 | Проанализировать профессионально-значимые источники информации с точки зрения основных аспектов: конфиденциальности, целостности и доступности. |
| Тема 1.2  Угрозы информационной безопасности в компьютерных системах | Содержание учебного материала | | 2 | 1 |
| 1 | Компьютерная система как объект защиты информации. | 2 |
| 2 | Понятие угрозы информационной безопасности в компьютерных системах. |
| 3 | Классификация и общий анализ угроз информационной безопасности в компьютерных системах. |
| 4 | Случайные угрозы информационной безопасности. |
| 5 | Преднамеренные угрозы информационной безопасности |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | | 3 | 4 |
|  | Самостоятельная работа студента | | 4 |  |
| 1 | Для выбранного объекта защиты информации (например, почтовый сервер, одиночно стоящий компьютер в бухгалтерии, телефонная база ограниченного пользования на электронных носителях и др.) провести анализ защищенности объекта по следующим пунктам: вид угроз, характер происхождения угроз, классы каналов несанкционированного получения информации, источники появления угроз, причины нарушения целостности информации, потенциально возможные злоумышленные действия; определить класс защиты информации. |
| Тема 1.3  Законодательный уровень информационной безопасности | Содержание учебного материала | | 6 | 2 |
| 1 | Значимость уровня в комплексном подходе. Меры законодательного уровня. |
| 2 | Законодательная и нормативно - правовая база РФ в области информатизации и защиты информации. |
| 3 | Ответственность за нарушение законодательства в информационной сфере. |
| 4 | Обзор зарубежного законодательства в области информационной безопасности. | 3 |
| Самостоятельная работа обучающихся | | 2 |  |
| 1 | Составить перечень основный понятий и определений, используемых в нормативно-правовых документах, касающихся информационной безопасности |
| Тема 1.4 Административный уровень информационной безопасности | Содержание учебного материала | | 2 | 2 |
| 1 | Основные понятия. |
| 2 | Политика безопасности. |
| 3 | Программа безопасности. |
| 4 | Синхронизация программы безопасности с жизненным циклом систем. |
| Тема 1.5  Процедурный уровень информационной безопасности | Содержание учебного материала | | 2 | 2 |
| 1 | Основные классы мер процедурного уровня. |
| 1 | 2 | | 3 | 4 |
|  | 2 | Управление персоналом. |  |  |
| 3 | Физическая защита. |
| 4 | Поддержание работоспособности. |
| 5 | Реагирование на нарушения режима безопасности. |
| 6 | Планирование восстановительных работ. |
| Самостоятельная работа обучающихся | | 4 |  |
| 1 | Проанализировать на основе определенного объекта (предприятия, организации, учреждения) поддержание групп мер процедурного уровня и дать оценку уровню поддержания безопасности |
| Тема 1.6 Программно-технический уровень информационной безопасности | Содержание учебного материала | | 2 | 2 |
| 1 | Основные понятия и меры уровня. |
| 2 | Особенности современных информационных систем. |
| 3 | Архитектурная безопасность. |
| **Раздел 2. Методы и средства обеспечения безопасности информации** | | | **54** |  |
| Тема 2.1  Методы и средства обеспечения безопасности информации | Содержание учебного материала | | 4 | 2 |
| 1 | Основные виды технических каналов утечки информации. Техника промышленного шпионажа. |
| 2 | Противодействие наблюдению. |
| 3 | Противодействие прослушиванию. |
| 4 | Методы и средства защиты от побочных электромагнитных излучений и наводок. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | | 3 | 4 |
| Тема 2.2  Защита информации от несанкционирова-нного доступа. | Содержание учебного материала | | 14 | 2 |
| 1 | Способы несанкционированного доступа к информации в компьютерных системах. |
| 2 | Характеристика средств защиты информации в компьютерных системах от несанкционированного доступа. |
| 3 | Идентификация и аутентификация пользователей: основные понятия, парольная аутентификация, виды паролей, биометрическая аутентификация. |
| 4 | Управление доступом: основные понятия, виды разграничения доступа, особенности дискреционного, мандатного и ролевого управления доступом |
| 5 | Защита программных средств от несанкционированного копирования и исследования. |
| 6 | Протоколирование и аудит: основные понятия, активный аудит. |
| 7 | Общая характеристика компонентов системы защиты операционной системы Windows 7 | 3 |
| 8 | Защита информации от несанкционированного доступа в операционных системах семейства Linux. | 2 |
| Практические работы (**1-3**) | | 6 |  |
| 1 | Изучение политики безопасности операционной системы Windows 7 |
| 2 | Управление шаблонами безопасности в Windows 7. |
| 3 | Разграничение полномочий и доступа к объектам операционной системы Linux |
| Лабораторные работы (**1-3**) | | 6 |
| 1 | Настройка параметров аутентификации Windows 7 |
| 2 | Назначение прав пользователей при произвольном управлении доступом в Windows 7 |
| 3 | Настройка параметров регистрации и аудита в Windows 7 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | | 3 | 4 |
|  | Самостоятельная работа студента | | 4 |  |
| 1 | Подготовка к лабораторным и практическим работам, оформление отчётов |
| Тема 2.3  Криптографические методы защиты информации | 1 | Развитие криптографических систем. Основные понятия криптологии. | 12 | 2 |
| 2 | Классификация криптографических средств. |
| 3 | Симметричные криптосистемы: DES и ее модификации, ГОСТ 28147-89, принципы их построения. |
| 4 | Асимметричные криптосистемы: однонаправленные функции, RSA, принципы построения. |
| 5 | Методы шифрования: замены, перестановки, аналитические, аддитивные, комбинированные. |
| 6 | Функция хэширования. |
| 7 | Электронная цифровая подпись и ее применение для контроля целстности программ и данных. |
| 8 | Компьютерная стеганография и ее применение. |
| 9 | Криптографический интерфейс приложений операционной системы Windows (CryptoAPI): принципы построения и особенности применения. |
| Практическая работа 4 | | 2 |  |
| 1 | Методы криптографического преобразования данных. |
| Лабораторная работа 4 | | 2 |
| 1 | Использование функций криптографического интерфейса (CryptoAPI) операционной системы Windows для защиты информации. |
| Самостоятельная работа студента | | 4 |
| 1 | Подготовка к лабораторной и практической работам, оформление отчётов |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | | 3 | 4 |
| **Раздел 3. Компьютерные вирусы и средства антивирусной защиты** | | | **20** |  |
| Тема 3.1  Вирусы как угроза информационной безопасности | Содержание учебного материала | | 2 | 1 |
| 1 | Общие сведения о компьютерных вирусах. |
| 2 | Классификация компьютерных вирусов. |
| 3 | Жизненный цикл вирусов. | 3 |
| 4 | Основные каналы распространения вирусов. |
| 5 | Вредоносные программы и их классификация. |
| Самостоятельная работа студента | | 4 |  |
| 1 | Разработать контролирующий, диагностический или демонстрационный материал по теме 3.1 (кроссворд, тест, ребусы, презентация и др.). |
| Тема 3.2  Средства антивируснойзащитых | Содержание учебного материала | | 4 | 1 |
| 1 | Методы и средства защиты от компьютерных вирусов. |
| 2 | Методы обнаружения и удаления вирусов. |
| 3 | Профилактика заражения вирусами компьютерных систем. |
| 4 | Программные закладки и методы защиты от них. | 2 |
| 5 | Антивирусные программные комплексы. | 3 |
| Практические работа 5-6 | | 4 |  |
| 1 | Антивирусные программные комплексы. |
| 2 | Восстановление зараженных файлов. Профилактика проникновения «троянских программ». |
| Самостоятельная работа обучающихся | | 6 |
| 1 | Подготовка к практическим работам, оформление отчётов |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | | 3 | 4 |
| **Раздел 4. Стандарты защищенности информации в компьютерных системах** | | | **14** |  |
| Тема 4.1  Стандарты и спецификации в области информационной безопасности | Содержание учебного материала | | 6 | 2 |
| 1 | Характеристика систем стандартизации в области защиты информации. | 3 |
| 2 | Оценочные стандарты и технические спецификации: «Оранжевая книга». |
| 3 | Информационная безопасность распределенных систем. Рекомендации X.800. |
| 4 | Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». |
| 5 | Европейские критерии безопасности информационных технологий. |
| 6 | Документы Гостехкомиссии России по защите информации. |
| Самостоятельная работа обучающихся | | 8 |  |
| 1 | Составить перечень понятий и определений, используемых в стандартах и спецификациях. |
| 1 | Для выбранного объекта защиты информации предложить анализ увеличения защищенности по следующим пунктам: определить требования к защите информации, определить факторы, влияющие на требуемый уровень защиты информации, выбрать или разработать способы и средства защиты информации, построить архитектуру систем защиты информации, сформулировать рекомендации по увеличению уровня защищенности. |

# 3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Реализация учебной дисциплины требует наличия учебного кабинета математических дисциплин.

Оборудование учебного кабинета:

* посадочные места по количеству обучающихся;
* рабочее место преподавателя;
* комплект наглядных пособий по разделам курса;
* комплект инструкционных карт для проведения практических занятий и лабораторных работ.

Технические средства обучения:

* компьютеры с лицензионным программным обеспечением, объединённые в локальную вычислительную сеть;
* мультимедиапроектор.
  1. **Информационное обеспечение обучения**

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

**Основные источники**

1. Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста [Текст] / К.Е. Климентьев. – М.: ДМК-Пресс, 2013. – 676 с.
2. Нестеров, С.А. Информационная безопасность [Текст]: учебник и практикум для академического бакалавриата / С.А. Нестеров. – М.: Издательство Юрайт, 2016. – 321 с.

**Дополнительные источники**

1. Аскеров, Т. М. Защита информации и информационная безопасность / Т.М. Аскеров. — М.: Издательство РЭА им. Плеханова, 2009. – 387 с.
2. Будко, В.Н. Информационная безопасность и защита информации. Конспект лекций / В.Н. Будко. – Воронеж: Издательство ВГУ, 2010. – 86 с.
3. Сычев, Ю.Н. Основы информационной безопасности / Ю.Н. Сычев. – М.: Евразийский открытый институт, 2010. – 328 с.

**Интернет-ресурсы:**

1. Википедия – свободная энциклопедия [Электронный ресурс] – Режим доступа:[http://ru.wikipedia.org](http://ru.wikipedia.org/) **–**;
2. ИНТУИТ. Национальный открытый университет. Проект [Издательства «Открытые Системы](http://www.osp.ru/)». [Электронный ресурс] – Режим доступа: http://Intuit.ru
3. Научная электронная библиотека; [Электронный ресурс] – Режим доступа: [www.elibrary.ru](http://www.elibrary.ru/) –
4. Новая электронная библиотека[Электронный ресурс] – Режим доступа: [www.newlibrary.ru](http://www.newlibrary.ru/) -;
5. Общероссийский математический портал[Электронный ресурс] – Режим доступа: [www.mathnet.ru](http://www.mathnet.ru/) –;
6. Федеральный портал российского образования[Электронный ресурс] – Режим доступа: [www.edu.ru](http://www.edu.ru/) –;
7. Электронная библиотека учебных материалов[Электронный ресурс] – Режим доступа: [www.nehudlit.ru](http://www.nehudlit.ru/) –.

14

# 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

|  |  |
| --- | --- |
| Результаты обучения (освоенные умения, усвоенные знания) | Формы и методы контроля и оценки результатов обучения |
| Умения: |  |
| выбирать средства обеспечения информационной безопасности информационной системы современного предприятия | экспертное оценивание выполнения практических занятий, лабораторных работ, самостоятельных работ |
| ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему | экспертное оценивание выполнения практических занятий, лабораторных работ |
| организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа | экспертное оценивание выполнения практических занятий, лабораторных работ |
| организовывать безопасную работу в Интернет и отправку почтовых сообщений в глобальной сети | экспертное оценивание выполнения лабораторной работы |
| использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов | экспертное оценивание выполнения практических занятий, самостоятельной работы |
| проводить базовые работы по профилактике нарушений информационной безопасности и построению защищенных информационных систем с использованием стандартных аппаратно-программных решений | экспертное оценивание выполнения практических занятий, лабораторных работ, самостоятельных работ |
| Знания: |  |
| вопросы административного и нормативно­-правового обеспечения защиты информации | экспертное оценивание выполнения самостоятельной работы, тестирование |
| основные системы защиты информации в России и в ведущих зарубежных странах | экспертное оценивание выполнения самостоятельной работы, тестирование |
| основные программно-аппаратные средства и методы защиты компьютерных систем | экспертное оценивание выполнения самостоятельных работ, тестирование |

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических и лабораторных занятий, тестирования, а также выполнения обучающимися внеаудиторной самостоятельной работы.

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.

|  |  |
| --- | --- |
| **Название ОК** | **Технология формирования ОК**  **(на учебных занятиях)** |
| 1 | 2 |
| ОК 1. Понимает сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес. | – овладевает первичными профессиональными навыками и умениями; |
| ОК 2. Организовывает собственную деятельность, выбирает типовые методы и способы выполнения профессиональных задач, оценивает их эффективность и качество. | – разбивает поставленную цель на задачи, подбирая из числа известных технологии (элементы технологий), позволяющие решить каждую из задач; |
| ОК 3. Принимает решения в стандартных и нестандартных ситуациях и несет за них ответственность. | – оценивает результаты деятельности по заданным показателям;  – выбирает способ разрешения проблемы в соответствии с заданными критериями и ставит цель деятельности; |
| ОК 4. Осуществляет поиск и использует информацию, необходимую для эффективного выполнения профессиональных задач, профессионального и личностного развития. | – задает критерии для сравнительного анализа информации в соответствии с поставленной задачей деятельности  делает вывод о применимости общей закономерности в конкретных условиях; |
| ОК 5. Использует информационно-коммуникационные технологии в профессиональной деятельности. | –демонстрирует навыки использования информационно-коммуникационныхтехнологий в профессиональной деятельности |
| ОК 6. Работает в коллективе и команде, эффективно общается с коллегами, руководством, потребителями. | –использует средства наглядности или невербальные средства коммуникации;  – извлекает из устной речи (монолог, диалог, дискуссия) фактическую и оценочную информацию, определяя основную тему, звучавшие предположения, аргументы, доказательства, выводы, оценки; |

|  |  |
| --- | --- |
| 1 | 2 |
| ОК 7. Берет на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. | –оценивает работу и контролирует работу группы;  – умеет представить результаты выполненной работы; |
| ОК 8. Самостоятельно определяет задачи профессионального и личностного развития, занимается самообразованием, осознанно планирует повышение квалификации. | – анализирует \ формулирует запрос на внутренние ресурсы (знания, умения, навыки, способы деятельности, ценности, установки, свойства психики) для решения профессиональной задачи; |
| ОК 9. Ориентируется в условиях частой смены технологий в профессиональной деятельности. | – выбирает технологии, применяемые в профессиональной деятельности; |
| ОК 10. Исполняет воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей). | –демонстрирует готовность к исполнению воинской обязанности. |