***Приложение II.11***

***к программе СПО 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»***

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**ОП.11 Корпоративная защита от внутренних угроз информационной безопасности**

**2021**

**Составитель:**

**Кислицин Никита Алексеевич, преподаватель ГБПОУ УКРТБ**

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| 1. ПАСПОРТ ПРОГРАММЫ 2. результаты освоения 3. структура и содержание 4. условия реализация программы 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ | 3  7  8  29  33 |

**1. ПАСПОРТ ПРОГРАММЫ**

|  |
| --- |
| **«Корпоративная защита от внутренних угроз информационной безопасности»** |

*название профессионального модуля*

**1.1. Цель и планируемые результаты освоения профессионального модуля**

Изучение предмета поможет в освоении компетенции **«Корпоративная защита от внутренних угроз информационной безопасности»** и подготовке к сдаче демонстрационного экзамена.

В результате изучения предмета студент должен освоить основной вид профессиональной деятельности «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты» и соответствующие ему профессиональные компетенции и общие компетенции:

Перечень профессиональных компетенций

|  |  |
| --- | --- |
| **Код** | **Наименование видов деятельности и профессиональных компетенций** |
| ВД 2. | *Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты* |
| ПК 2.1. | Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей. |
| ПК 2.2. | Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях. |
| ПК 2.3. | Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями. |

В результате освоения предмета студент должен:

|  |  |
| --- | --- |
| Иметь практический опыт в | - установка, настройка, испытания и конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС;  - поддержание бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС;  - защита информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты в соответствии с предъявляемыми требованиями. |
| уметь | - выявлять и оценивать угрозы безопасности информации в ИТКС;  - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;  -проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  -проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  -выявлять и оценивать угрозы безопасности информации в ИТКС;  - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;  -выявлять и оценивать угрозы безопасности информации в ИТКС;  -настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;  -проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  *-проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации российского производства;*  *-проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации российского производства.* |
| знать | - способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее;  -типовых программных и программно-аппаратных средств защиты информации в ИТКС;  -криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;  -возможных угроз безопасности информации в ИТКС;  -способов защиты информации от НСД и специальных воздействий на нее;  -порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  -организации и содержания технического обслуживания и ремонта программно-аппаратных (в том числе криптографических) средств защиты информации;  -порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации;  -возможных угроз безопасности информации в ИТКС;  - способов защиты информации НСД и специальных воздействий на нее;  -типовых программных и программно-аппаратных средств защиты информации в ИТКС;  -криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;  -порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации  *-программные и программно-аппаратные средства защиты информации в ИТКС российского производства;*  *-криптографические средства защиты информации конфиденциального характера, которые применяются в ИТКС на основе российских стандартов;*  *-порядок и правила ведения документации планово предупредительных работ на программные и программно-аппаратные (в том числе криптографические) средства защиты информации.* |

**1.2. Количество часов, отводимое на освоение предмета**

Всего часов – 88 часов, в том числе:

- 88 часов вариативной части, направленных на усиление обязательной части программы.

**2. СТРУКТУРА и содержание УЧЕБНОЙ ДИСЦИПЛИНЫ**

**2.1. Структура профессионального модуля**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Коды профессиональных компетенций** | **Наименования разделов профессионального модуля[[1]](#footnote-1)\*** | **Суммарный объем нагрузки, час** | **Объем профессионального модуля, час** | | | | | | |
| **Обучение по МДК** | | | | **Практика** | | **Промежуточная аттестация** |
| **Всего,**  часов | **в т.ч. лабораторные работы и практические занятия,**  часов | **в т.ч., курсовая работа (проект),**  часов | **Самостоятельная работа** | **Учебная,**  часов | **Производственная (по профилю специальности),**часов |
| **ПК 2.1**  **ПК 2.2** | **Раздел 1.** Корпоративная защита от внутренних угроз информационной безопасности | **88** | **88** | 40 |  | **8** |  |  |  |
|  | **Всего:** | **88** | **88** | 40 |  | **8** |  |  |  |

# **3.2. Тематический план и содержание предмета (ПМ) «Корпоративная защита от внутренних угроз информационной безопасности»**

VI семестр

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Наименование разделов и тем предмета(ПМ), междисциплинарных курсов (МДК)** | | | **Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)** | | **Объем часов** |
| **1** | | | **2** | | **3** |
| **Раздел 1.** Корпоративная защита от внутренних угроз информационной безопасности | | | | | **88** |
| **Тема 1.1**  Изучение серверных и десктопных версий  ОС Linux | | | **Содержание** | | **34** |
| 1 | **Linux. QNX и другие операционные системы.** | 2 |
| 2-3 | **Bash, структуры, пути.**  Использование команд Linux  Управление аккаунтами в Linux | 4 |
| 4-5 | **Создание ссылок и удаление файлов.**  Использование джокеров | 4 |
| 6-7 | **Регулярные выражения**  FHS и поиск файлов  Стандарт иерархии файловой системы | 4 |
| 8 | **Модули ядра**  Системная и сетевая документация  Типы системной документации в Linux  Модель прав доступа в Linux | 2 |
| **Практические занятия** | | **18** |
| 1 | Установка виртуальных машин серверной и десктопной версии ОС Linux | 2 |
| 2 | Знакомство с оболочкой Linux | 2 |
| 3 | Работа с текстовыми файлами в интерфейсе командной строки | 2 |
| 4 | Серверы Linux | 2 |
| 5 | Поиск файлов журналов | 2 |
| 6 | Навигация в файловой системе Linux и настройка полномочий | 2 |
| 7 | Трассировка маршрута | 2 |
| 8 | Общие сведения о программе Wireshark | 2 |
| 9 | Дисковая подсистемой и RAID | 2 |
| **Тема 1.2** | | | **Содержание** | | **40** |
| 1 | Протокол TCP/IP | 2 |
| 2 | Служба DNS | 2 |
| 3 | Служба каталогов Active Directory. Служба файлов и печати | 2 |
| 4 | Сетевые протоколы и службы. Служба резервного копирования | 2 |
| 5 | Службы терминалов. Мониторинг | 2 |
| 6 | Модель OSI | 2 |
| 7 | Физический, канальный и сетевой уровень | 2 |
| 8 | Транспортный, сеансовый, предоставления и прикладной уровень | 4 |
| **Практические занятия** | | 20 |
| 9 | Расчет IPv4, IPv6 сетей | 2 |
| 10-11 | Поднятие роли DNS в домене | 4 |
| 12 | Поднятие роли AD в домене | 2 |
| 13 | Репликация домена | 2 |
| 14 | Ввод компьютера в домен | 2 |
| 15-16 | Создание пользователей | 4 |
| 17 | Работа с групповыми политиками | 2 |
| 18 | Настройка общих папок в домене | 2 |
| **Тема 1.3**  Обеспечение безопасности компьютерных систем и сетей. Технологии Data Leakage Prevention (DLP). | | | **Содержание** | | **34** |
| 1 | **Защита информации от внутренних угроз информационной безопасности.** Выявление утечек с использованием технологии Data Leakage Prevention (DLP). Теория и практика применения DLP-систем. | 2 |
| 2 | **Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.** | 2 |
| 3 | **Установка DLP IWTM в виртуальном окружении. Режимы port mirroring и proxy.** | 2 |
| 4 | Конфигурирование DLP IWTM  Исправление типовых неисправностей. | 2 |
| 5 | **Технологии агентского мониторинга**  Назначение агентского мониторинга. Установка и настройка агентского мониторинга. Интерфейс консоли DLP IWDM. Работа в консоли управления агентом | 2 |
| 6 | **Политики агентского мониторинга, особенности их настройки.** Создание и проверка политик. Создание политик защиты на агентах; Фильтрация событий;  Настройка совместных событий агентского и сетевого мониторинга; Работа с носителями и устройствами; Работа с файлами; Контроль приложений; Исключение из событий перехвата. | 2 |
| 7 | **Разработка политик безопасности, анализ выявленных инцидентов** | 2 |
| 8 | **Разработка и тестирование политик в системе DLP IWTM.** Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии; Работа со сводками, виджетами, сводками; Работа с персонами; Работа с объектами защиты; Провести имитацию процесса утечки конфиденциальной информации в системе; Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. Работа с категориями и терминами; Использование регулярных выражений; Использование морфологического поиска; • Работа с графическими объектами; Работа с выгрузками и баз данных; Работа с печатями и бланками; Работа с файловыми типами; | 2 |
| 9 | **Мониторинг трафика.** Проверка применения политик 4-х видов: трафик, персоны, буфер обмена, движение файлов. Работа с краулером. | 2 |
| **Практические занятия** | | **16** |
| 1 | Установка, конфигурирование и  устранение неисправностей в системе  корпоративной защиты от внутренних угроз | 2 |
| 2-3 | Разработка политик безопасности в  системе корпоративной защиты информации от  внутренних угроз | 4 |
| 4 | Поиск и предотвращение  инцидентов. Технологии анализа сетевого  трафика в системе корпоративной защиты  информации от внутренних угроз | 2 |
| 5-6 | Технологии агентского мониторинга | 4 |
| 7-8 | Анализ выявленных инцидентов | 4 |
| **Примерная тематика домашних заданий** | | | | |  |
| 1.1. | 1 Чтение и анализ литературы:[3]с.223-229  2 Чтение и анализ литературы:[3]с.172-176  3 Чтение и анализ литературы:[3] с.176-186  4 Чтение и анализ литературы:[3] с.188-196  5 Чтение и анализ литературы:[8] с. 1-7  6 Чтение и анализ литературы:[8] с.11-49  7 Чтение и анализ литературы:[8] с.50-58  8 Чтение и анализ литературы:[8] с.29-42 | | | |
| 1.2. | 1 Чтение и анализ литературы:[3] с.229-231  2 Чтение и анализ литературы:[3] с.231-239  3 Чтение и анализ литературы:[3] с.231-239  4 Изучение конспекта лекций: [3]с.235-236  5 Изучение конспекта лекций: [3]с. 488-491  6 Чтение и анализ литературы:[3] с.239-241  7 Чтение и анализ литературы:[3] c.262-271, [9] c. 77-84  8 Чтение и анализ литературы:[3] с.271-282, [9] c. 84-88  9 Чтение и анализ литературы:[3] с.282-291  10 Чтение и анализ литературы:[9] c. 115-120, моделирование ситуаций | | | |
| 1.3. | 1 Чтение и анализ литературы:[3] c.40-42  2 Чтение и анализ литературы:[3] c.65-71  3 Чтение и анализ литературы:[3] c.293-307  4,5 Чтение и анализ литературы:[3] c.323-324  6,7 Чтение и анализ литературы:[3] c.324-333  8,9 Чтение и анализ литературы:[3] c.333-341  10,11 Чтение и анализ литературы:[3] c. 346-362  12,13 Чтение и анализ литературы:[3] c.380-416 | | | |
| **Самостоятельная работа при изучении раздела**  Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем).  Подготовка к практическим работам с использованием методических рекомендаций преподавателя.  Оформление практических работ, отчетов и подготовка к их защите. | | | | | **8** |
| **Примерная тематика домашних заданий** | | | | |  |
| 1.4 | | 1,2 Чтение и анализ литературы [3] с.171-189  3 Чтение и анализ литературы [3] с.189-191  4 Чтение и анализ литературы [3] с.191-197  5,6Чтение и анализ литературы [3] с.199-211  7,8 Чтение и анализ литературы [3] с.2-11-221  9,10 Чтение и анализ литературы [3] с.222-234  11,12 Чтение и анализ литературы [3] с.236-243  13,14 Чтение и анализ литературы [3] с.243-252  15,16 Чтение и анализ литературы [3] с.252-277 | | |
| 1.5 | | 1 Чтение и анализ литературы:[3] c.427-435  2 Чтение и анализ литературы:[3] c.436-439  3,4 Чтение и анализ литературы:[3] c.439-453  5 Чтение и анализ литературы:[3] c.453-464, 464-481  6 Чтение и анализ литературы [3] с.481-492  7 Чтение и анализ литературы [3] с.492-495  8 Чтение и анализ литературы [3] с.496-497  9 Чтение и анализ литературы [3] с.498-502  10 Чтение и анализ литературы [3] с.502-505  11 Чтение и анализ литературы [3] с.505-511  12 Чтение и анализ литературы [3] с.511-512 | | |  |
| 1.6 | | 1 Чтение и анализ литературы:[3] c.481-496  2 Чтение и анализ литературы:[3] c.496-501  3 Чтение и анализ литературы:[3] c.501-507 | | |  |

# **3.условия реализации программы ПРЕДМЕТА**

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

Реализация программы модуля предполагает наличие учебной лаборатории программно-аппаратных средств обеспечения информационной безопасности.

Оборудование учебного кабинета и рабочих мест кабинета:

- посадочные места по количеству обучающихся;

- рабочее место преподавателя;

- комплект учебно-методических документации;

- дидактические материалы.

- учебно-наглядные пособия по дисциплине «Информационная безопасность и защита информации»:

- плакаты:

- «Модель информационной безопасности»;

- «Технические каналы утечки информации»;

- «Односторонне функции шифрования»;

- «Модель угроз информационной безопасности»;

- «Сертификаты открытых ключей»

- презентации:

- «Технические средства защиты информации»;

- «Инженерно технические средства защиты информации»;

- «Средства криптографической защиты информации »;

- учебный фильм:

- «Зашифрованная война»

- мультимедиапроектор, компьютер преподавателя;

Оборудование лаборатории программно-аппаратных средств обеспечения информационной безопасности:

Технические средства обучения:

- персональные компьютеры (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i5, оперативная память DDR4 объемом не менее 16 Гб; HD 1000 Gb видеокарта, БП 650 Ватт), объединенные в учебную локально- вычислительную сеть с выходом в сеть Интернет, по количеству обучающихся с лицензионным программным обеспечением: ОС Windows XP, Windows Server 2003, OC Unix;

- система InfoWatch;

- монитор с возможностью поворота экрана не менее 90 градусов, не менее 23,8 дюйма, HDMI, USB;

- криптошлюз ПАКViPNetCoordinator HW100;

- коммутатор L2 уровень, 16 портов Ethernet стандарта 1000BASE-T;

- маршрутизатор 4 порта Ethernet стандарта 1000BASE-T;

**-** АПМДЗ Соболь PCI-E.

- учебно-лабораторный комплекс «Криптон» (Платы «Криптон-замок», аппаратные абонентские и сетевые шифраторы, программное обеспечение);

- учебно – лабораторный комплекс беспроводной сети Wi-Fi;

-лабораторное измерительное оборудование:

- осциллограф -2 шт.;

- частотомер – 2 шт.;

- генератор – 1 шт.;

- мультиметр – 4 шт.;

- источник питания – 6 шт.;

- паяльная станция – 2 шт.;

- демонтажная станция -1 шт.;

- анализатор поля – 1 шт.;

- измеритель электромагнитного поля – 1 шт.;

- детектор излучений -1 шт.;

- индикатор СВЧ -1шт;

- тестер кабельных линий -1 шт.;

- лабораторные стенды:

- «Изучение системы видеонаблюдения»;

- «Изучение систем контроля доступа»;

-«Изучение беспроводной системы охранно-пожарной сигнализации»;

- «Светочувствительная сигнализация»

- «Микроконтроллерное устройство управления исполнительными блоками для режимных объектов»

- «Микропроцессорное автоматическое устройство управления системой принудительного охлаждения телекоммуникационной стойкой аппаратуры по 4 каналам измерения в реальном масштабе времени»

- «Изучение биометрических систем контроля доступа»

- «Структурированные кабельные системы NIKOMAX»

Реализация программы модуля предполагает обязательную учебную практику.

**3.2. Информационное обеспечение обучения**

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

Основные источники:

1. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие/ Фороузан Б.А.; пер. с англ. Под ред.А.Н. Берлина. - М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2015.-784с.:ил.,табл.-(Основы информационных технологий).2. Максименко В.Н., Афанасьев В.В., Волков Н.В. Защита информации в сетях сотовой подвижной связи/ Под ред. доктора техн. Наук, профессора О.Б. Макаревича. – М.: Горячая линия – Телеком, 2014. -360с.: ил.

3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства –М.: ДМК Пресс, 2016. – 544с.:ил.

4. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. –СПб.:2016.-272с.:ил.

5. Васильков А.В., Васильков А.А., Васильков И.А Информационные системы и их безопасность: учебное пособие –М.: ФОРУМ, 2017.-528с.- (Профессиональное образование)

6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Техническая защита информации. Учебник для вузов -5-е изд., перераб. и доп. – М.: - Горячая линия – Телеком, 2015. – 616с:ил.

7.Романов О.А. Организационное обеспечение информационной безопасности: учебник для студентов высш. учеб. заведений –М.: Издательский центр «Академия», 2015. – 192с.

8. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябов Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2016. – 363 с.

9. InfoWatch Traffic Monitor Руководство пользователя – М.: ЗАО "ИнфоВотч", 2017. – 178 с.: ил..

Дополнительные источники:

1 Руководство администратора Криптон-замок

2. Руководство администратора ППКОП «Астра»

3. Руководство администратора КТМ-256

4. Учебное пособие Структурированная кабельная система NIKOMAX»

Интернет ресурсы:

1. Электронно-библиотечная система [Электронный ресурс] – режим доступа: http:// www.znanium.com/ (2021).

2. http://www.fstec.ru сайт ФСТЭК РФ

3. http://www.ancad.ru сайт компании АНКАД

4. https://www.cryptopro.ru/ сайт компании КриптоПро

5. https://infotecs.ru/ сайт ОАО «ИнфоТеКС»

6. Центр оказания образовательных услуг и подготовки специалистов в области информационной безопасности и эксплуатации средств защиты информации ViPNet. [Электронный ресурс] – режим доступа: https://edu.infotecs.ru/learning/ (2021)

# **4. Контроль и оценка результатов освоения предмета**

|  |  |  |
| --- | --- | --- |
| **Код и наименование**  **профессиональных и общих компетенций, формируемых в рамках модуля** | **Критерии оценки** | **Методы оценки** |
| **Раздел модуля 1 Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты** | | |
| ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей. | - выявлять и оценивать угрозы безопасности информации в ИТКС;  - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;  - проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; | Экспертное наблюдение |
| ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях. | - выявлять и оценивать угрозы безопасности информации в ИТКС;  - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации; | Экспертное наблюдение |
| ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями. | - выявлять и оценивать угрозы безопасности информации в ИТКС;  - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;  - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; | Экспертное наблюдение |
| ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. | - обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;  - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач; | Экспертное наблюдение  Экзамен |
| ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. | - использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач; | Экспертное наблюдение  Экзамен |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие. | - демонстрация ответственности за принятые решения;  - обоснованность самоанализа и коррекция результатов собственной работы; | Экспертное наблюдение  Экзамен |
| ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. | - взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик;  - обоснованность анализа работы членов команды (подчиненных); | Экспертное наблюдение  Экзамен |
| ОК 09. Использовать информационные технологии в профессиональной деятельности. | - эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту; | Экспертное наблюдение  Экзамен |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранных языках | - эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке. | Экспертное наблюдение  Экзамен |

1. [↑](#footnote-ref-1)