ДЕПАРТАМЕНТ СМОЛЕНСКОЙ ОБЛАСТИ ПО ОБРАЗОВАНИЮ И НАУКЕ
областное государственное бюджетное профессиональное образовательное учреждение
«Смоленская академия профессионального образования»
(ОГБПОУ СмолАПО)

УТВЕРЖДАЮ
Директор ОГБПОУ СмолАПО
_____М. В. Белокопытов

ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.09 Основы сетевой безопасности

Смоленск
2019 г.

Программа профессионального модуляПМ.09Основы сетевой безопасностивходит в состав инвариантной части основной профессиональной образовательной программы, разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 09.02.07 Информационные системы и программирование по программе углубленной подготовки

Организация разработчик: ОГБПОУ СмолАПО

Разработчик:

Кудрявцева Т.В. - преподаватель ОГБПОУ СмолАПО

Рассмотрено на заседании кафедры Информационных технологий

Протокол № 1 от 30.08.2019 г.

Рекомендовано к утверждению научно-методическим советом ОГБПОУ СмолАПО

Протокол № 1 от 31.08.2019 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.09 Основы сетевой безопасности

1.1. Область применения программы

Программа профессионального модуля ПМ.09 Основы сетевой безопасностивходит в состав вариативной части основной профессиональной образовательной программы, разработана в соответствии с ФГОС по специальности СПО09.02.07 Информационные системы и программирование по программе углубленной подготовкив части освоения вида профессиональной деятельности (ВПД):**Обеспечение информационной безопасности компьютерной сети и ее ресурсов**исоответствующих профессиональных компетенций (ПК):

- производить оценку надежности и безопасности компьютерной сети;
- применять современные технологии и средства обеспечения информационной безопасности компьютерной сети;
- обеспечивать защиту программного обеспечения компьютерных систем.

Программа профессионального модуля может быть использована в дополнительном образовании по направлению подготовки 09.02.07 Информационные системы и программирование по программе углубленной подготовкии в профессиональной подготовке по профессиям:

16199Оператор электронно – вычислительных и вычислительных машин,

26965 Техник вычислительного (информационно-вычислительного) центра,

230103.04 Наладчик аппаратного и программного обеспечения,

230103.03 Наладчик компьютерных сетей.

1.2. Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- администрирования сетевого экрана;
- создания политик для межсетевого экрана с возможностями NAT;
- применения систем обнаружения и предотвращения проникновений;
- создания GRE-туннеля;
- управления учетными записями;

уметь*:*

- осуществлять сегментирование сети с помощью управляемого коммутатора;
- настраивать альтернативные маршруты с использованием статической маршрутизации;
- применять алгоритмы симметричного и ассиметричного шифрования;
- настраивать соединение двух локальных сетей с использованием протоколов L2TP и GRE/IPSec;

знать*:*

- типы сетевых атак;
- основные принципы организации безопасной ИТ-инфраструктуры;
- технологии сегментации сетей;
- типы межсетевых экранов и их возможности;
- особенности топологии сети с межсетевым экраном;
- назначение, типы и возможности систем обнаружения и предотвращения проникновений;
- способы создания альтернативных маршрутов доступа в интернет;
- понятие приоритезации трафика;
- методы криптографической защиты;
- понятие виртуальной чети;
- назначение протоколов L2TP, SSL/TLS,IPSec, RADIUS и LDAP;
- способы управления учетными записями.

1.3. Рекомендуемое количество часов на освоение примерной программы профессионального модуля:

Всего – 332часов, в том числе:

- максимальной учебной нагрузки обучающегося – 260 часа, включая:
  - обязательной аудиторной учебной нагрузки обучающегося – 174 часа;
  - самостоятельной работы обучающегося – 86 часов,
- производственной практики – 72 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности **Обеспечение информационной безопасности компьютерной сети и ее ресурсов**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 9.1	Производить оценку надежности и безопасности компьютерной сети
ПК 9.2	Применять современные технологии и средства обеспечения информационной безопасности компьютерной сети
ПК 2.4	Реализовывать методы и технологии защиты информации в базах данных
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2	Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.
ОК 4	Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.
ОК 6	Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, планировать повышение квалификации.
ОК 9	Быть готовым к смене технологий в профессиональной деятельности.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

ПМ.09 Основы сетевой безопасности

Коды профессиональных компетенций	**Наименования разделов профессионального модуля**	**Всего часов** *(макс. учебная нагрузка и практики)*	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная (по профилю специальности),** часов *(если предусмотрена рассредоточенная практика)*
			Всего, часов	**в т.ч. практические занятия,** часов	**в т.ч., курсовая работа (проект),** часов	**Всего,** часов	**в т.ч., курсовая работа (проект),** часов		
ПК 9.1, ПК 9.2ПК 5.4	Раздел 1. Межсетевые экраны	170	90	34	-	44	-	-	36
ПК 9.1, ПК 9.2, ПК 5.4	Раздел 2. Технологии туннелирования	162	84	30	-	42	-	-	36
	Производственная практика (по профилю специальности), часов								72
	Всего:	**332**	**174**	**64**	-	**86**	-	-	**72**

3.2. Содержание обучения по профессиональному модулю ПМ.09 Основы сетевой безопасности

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)		Объем часов	Уровень освоения
1	2		3	4
ПМ.09 Основы сетевой безопасности			**332**	
Раздел 1 ПМ.09 Межсетевые экраны			**134**	
МДК09.01 Межсетевые экраны			**134**	
Тема 1.1Основные принципы создания надежной и безопасной ит-инфраструктуры	**Содержание**		**14**	3
	1	Введение. Классификация сетевых атак		
	2	Триада безопасной ИТ-инфраструктуры – Конфиденциальность, Целостность, Доступность.		
	3	Гарантирование выполнения. Анализ рисков.		
	4	Аутентификация и управление идентификациями. Управление доступом.		
	5	Обеспечение отчетности. Гарантирование доступности.		
	6	Управление конфигурациями. Управление инцидентами.		
	7	Использование третьей доверенной стороны. Криптографические механизмы безопасности.		
	Практическая работа		**8**	
	1-2	Основы администрирования межсетевого экрана		
	3-4	Соединение двух локальных сетей, расположенных за межсетевыми экранами		
Тема 1.2 Сегментирование сетей на канальном уровне	**Содержание**		**8**	3
	1	Использование технологии VLAN для создания подсетей		
	2	Стандарт IEEE 802.1Q		
	3	Типовая топология сети с использованием VLAN		
	4	VLAN на основе портов		
	Практическая работа		**6**	
	1-2	Сегментирование подсетей с использованием управляемых коммутаторов		
	3	Сегментирование подсетей на основе port-based VLAN		
Тема 1.3 Межсетевые экраны	**Содержание**		**22**	3

	1-3 (2 и3 – 2 сем)	Введение. Технологии межсетевых экранов		
	4-5	Политика межсетевого экрана		
	6-7	Межсетевые экраны с возможностями NAT		
	8-9	Топология сети при использовании межсетевых экранов		
	10-11	Планирование и внедрение межсетевого экрана		
	Практическая работа		**10**	
	1	Создание политики без проверки состояния		
	2-3 (2сем)	Создание политик для традиционного (или исходящего) NAT		
	4-5	Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing		
Тема 1.4 Системы обнаружения и предотвращения проникновений	**Содержание**		**8**	3
	1	Введение. Основное назначение IDPS. Способы классификации IDPS.		
	2	Выбор IDPS. Дополнительные инструментальные средства.		
	3	Требования организации к функционированию IDPS. Возможности IDPS.		
	4	Развертывание IDPS. Сильные стороны и ограниченность IDPS. Выходные данные IDPS.		
	Практическая работа		**4**	
	1	Антивирусное сканирование		
	2	Обнаружение и предотвращение вторжений		
Тема 1.5 Приоритезация трафика и создание альтернативных маршрутов	**Содержание**		**4**	3
	1	Создание альтернативных маршрутов доступа в интернет		
	2	Приоритезация трафика		
	Практическая работа		**6**	
	1	Создание альтернативных маршрутов с использованием статической маршрутизации		
	2	Ограничение полосы пропускания трафика		
	3	Ограничение полосы пропускания P2P-трафика с использованием IDP		

Самостоятельная работа при изучении раздела 1 1. Подготовка рефератов, сообщений, презентаций. 2. Построение схем, заполнение таблиц. 3. Составление опорного конспекта. 4. Работа с электронными информационными ресурсами и ресурсами Internet. 5. Решение вариативных задач и упражнений.			**44**	
Раздел 2 ПМ.09 Технологии туннелирования			**126**	
МДК 09.02 Технологии туннелирования			**126**	
Тема 2.1 Криптографические механизмы безопасности	**Содержание**		**14**	2
	1-3	Алгоритмы симметричного шифрования		
	4-5	Хэш-функции		
	6	Алгоритмы асимметричного шифрования		
	7	Инфраструктура Открытого Ключа		
Тема 2.2 Технологии туннелирования	**Содержание**		**30**	3
	1-2	Протокол GRE.		
	3-4	Виртуальные частные сети. Протоколы канального уровня.		
	5-7 (6-7 2 сем)	Виртуальные частные сети. Семейство протоколов IPSec		
	8-9	Виртуальные частные сети. Совместное использование протоколов L2TP и IPSec.		
	10	Протокол SSL/TLS. Обзор.		
	11	Протокол SSL/TLS Протокол Записи.		
	12-13	Протокол SSL/TLS. Протокол Рукопожатия.		
	14-15	Протокол SSL/TLS. Добавление дополнительных возможностей в протокол		
	Практическая работа		**22**	
	1	Соединение двух локальных сетей GRE-туннелем		
	2	Соединение двух локальных сетей протоколом IPSec в туннельном режиме, аутентификация с использованием общего секрета		
	3	Использование аутентификации по стандарту XAuth в протоколе IPSec		
	4	Соединение двух межсетевых экранов протоколом IPSecв транспортном режиме, аутентификация с использованием общего секрета		

	5	Использование преобразования NAT в протоколе IPSec		
	6	Использование протокола DPD в протоколе IPSec		
	7	Соединение двух локальных сетей протоколом L2TP, аутентификация с использованием общего секрета		
	8 (2 сем)	Соединение двух локальных сетей протоколом GRE/IPSecв транспортном режиме		
	9	Соединение двух локальных сетей протоколом L2TP/IPSecв транспортном режиме		
	10-11	Соединение двух локальных сетей протоколом L2TP/IPSecв транспортном режиме, для одной из локальных сетей используется NAT		
Тема 2.3 Аутентификация и хранение учетных записей	**Содержание**		**10**	2
	1-3	Топология сети. Протокол RADIUS.Основные понятия. Аутентификация RADIUS. Аккаунтинг RADIUS.		
	4-5	Протокол LDAP.Введение. Основные характеристики LDAP		
	Практическая работа		**8**	
	1	Использование локальной БД для хранения учетных записей		
	2	Использование сервера RADIUS для хранения учетных записей		
	3	Использование сервера LDAP/MS AD для хранения учетных записей		
	4	Аутентификация доступа к ресурсам с использованием браузера		
Самостоятельная работа при изучении раздела 2 1. Подготовка рефератов, сообщений, презентаций. 2. Построение схем, заполнение таблиц. 3. Составление опорного конспекта. 4. Работа с электронными информационными ресурсами и ресурсами Internet. 5. Решение вариативных задач и упражнений.			**42**	
Виды работ по практикепо профилю специальности – анализ структуры и состава вычислительной сети; – выявление рисков с точки зрения защищенности физического оборудования, программного обеспечения вычислительной системы, обеспечения безопасности ее ресурсов; – составление перечня мероприятий по повышению уровня безопасности; – реализация мер по обеспечению информационной безопасности вычислительной сети и ее ресурсов с применением технологий: сегментирования сети, межсетевого экранирования, туннелирования и др.			**72**	

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).

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация профессионального модуля предполагает наличие мастерская «Кибер-безопасности»,оснащенная следующим оборудованием и программным обеспечением:

– Персональный компьютер в сборе: Processor - AMD Ryzen X8 R7-1700, DDR4 DIMM 32Гб, Видеокарта - ASUS GeForce GTX 1650 PHOENIX OC [PH-GTX1650-04G], SD накопитель A-DATA S11 Pro AGAMMIXS11P-512GT-C 512 Гб;

– Компьютерный монитор AOC 24" G2460VQ6;

– Клавиатура USB CBR KB 107;

– Компьютерная мышь USB CBR CM-302;

– Источник бесперебойного питания Powercom UPS RPT-800A EURO;

– Сервер [2U / 2 x Intel Xeon Silver 4210R (2.4GHz,10C) / 8 x 32Gb DDR4 2933, ECC R(24up) / 4x960Gb SSD SATA / 4 x 10GE / 2 x 800w;

– Управляемый Коммутатор Cisco WS-C2960L-48;

– Коммутатор L3 WS-C3650-24;

– Телевизор 50” LED Haier LE50K5500TF;

– Флипчат электронный SMART kapp 42;

– Интерактивная доска ScreenMedia;

– Проектор CASIO XJ-V110W с потолочным креплением и коммутацией;

– МФУ Canon i-SENSYS MF426dw;

– USB-токен JaCarta-2 PKI/ГОСТ (XL) JC-MediaKit-4 - "ПКJaCarta – MediaKit,

– РутокенЭЦП 2.0 64 кб;

– RDS-01 USB считывательключей Dallas Touch Memory (iButton);

– DS1996 сизогнутымбрелоком - электронныйключDallasTouchMemory (IButton);

– FindkeyHamster III (HFDU06S) - настольный биометрический считыватель;

– Установочный комплект. Средство защиты информации SecretNetStudio 8;

– Установочный комплект. Средство защиты информации vGate R2;

– Дистрибутив СКЗИ КриптоПро CSP версии 5.0 КС1 и КС2 на DVD;

– Формуляры DallasLock 8.0-К. Право на использование** (СЗИ НСД.СКН); Бессрочная лицензия DallasLock 8.0. Сертифицированный комплект для установки;

– Программное обеспечение клиентского доступа к виртуальным машинам AcademicVMwareWorkstation 15 ProforLinuxandWindows;

– СистемавиртуализацииVMWare ESXI 7.0, VMWare Workstation Pro, Oracle VirtualBox;

– ПО операционная система Windows 10 с интегрированной программной платформой .NET Framework, 4.8;

– ПО для просмотра документов в формате PDF AdobeReader DC;

– ПО для архивации 7-Zip;

– ПО офисный пакет MicrosoftOffice 2019;

– СистемавиртуализацииVMWare ESXI 7.0, VMWare Workstation Pro, Oracle VirtualBox;

– Антивирусное программное обеспечение KasperskyEndpointSecurity.

Каждое рабочее место, оснащено персональным компьютером с высокоскоростным доступом к сети Интернет.

4.2. Информационное обеспечение обучения
Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:

Основные источники (печатные издания):

1. Компьютерные сети: учебное пособие под ред. М. В. Максимов, И. И. Попов. – М., 2017

Основные источники (электронные издания):

1. Учебный курс D-Link «Основы сетевых технологий», 2015
2. Учебный курс D-Link «Основы сетевой безопасности. Межсетевые экраны», 2015
3. Учебный курс D-Link «Основы сетевой безопасности. Технологии туннелирования», 2015
4. Лабораторные работы к учебному курсу D-Link «Основы сетевой безопасности. Межсетевые экраны», 2015
5. Лабораторные работы к учебному курсу D-Link «Основы сетевой безопасности. Технологии туннелирования», 2015

Дополнительные источники (печатные издания):

1. Новожилов Е.О. Компьютерные сети (4-е изд., стер.) учеб. Пособие. - М.: Академия, 2014

2. Олифер В. Г. Компьютерные сети,. Принципы, технологии, протоколы: учебное пособие для студентов вуза, обучающихся по направлению "Информатика и вычислительная техника" / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - М. [и др.]: Питер , 2012. - 944 с.

Электронные Интернет-ресурсы

1. Электронный учебник по компьютерным сетям. Форма доступа: http://kafvt.narod.ru/Osia/frameset.htm

2. Электронные ресурс КОМПЬЮТЕРНЫЕ СЕТИ. Форма доступа: http://firm.trade.spb.ru/serp/net/main_net.htm

Программное обеспечение

1. Операционные системы.
2. Системы антивирусной защиты
3. Специализированное ПО

4.3. Общие требования к организации образовательного процесса

Программа профессионального модуля ПМ.09 Основы сетевой безопасности реализуется в течение2-х семестров пятого курса обучения (9 и 10 семестры).

Освоению данного модуля предшествует изучение дисциплин общего гуманитарного и социально-экономического, математического и естественнонаучного, общепрофессионального циклов, таких как: Операционные системы, Архитектура компьютерных систем, Информационная безопасность, Технологии коммутации и маршрутизации современных сетей Ethernet, а так же МДК 02.01 Инфокоммуникационные системы и сети.

В процессе обучения студентов основными формами являются: аудиторные занятия, включающие лекции и практические занятия, а так же самостоятельная работа обучающегося. Тематика лекций и практических занятий соответствует содержанию программы профессионального модуля.

Обязательным условием допуска к производственной практике (по профилю специальности) в рамках данного профессионального модуля является освоение учебной практики в рамках профессионального модуля.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение попрофессиональному модулю**:** наличие высшего профессионального образования, соответствующего профилю модуля и специальности 09.02.03Программирование в компьютерных системах.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: высшее инженерное образование, соответствующее профилю модуля.

Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным.

Прохождение стажировки на промышленных предприятиях и производственно-коммерческих организациях не реже 1 раза в 3 года.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

5.1 Контроль и оценка результатов освоения профессиональных компетенций

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 9.1 Производить оценку надежности и безопасности компьютерной сети	– Правильность проведения анализа структуры и состава ИТ- инфраструктуры; – Полнота в перечислении направлений анализа защищенности ИТ-инфраструктуры; – Полнота и точность в определении рисков ИТ-инфраструктуры сточки зрения сетевой безопасности;	Входной контроль: - проверочная работа на знание теоретических вопросов. Текущий контроль: −устный и письменный опрос; −тестирование по темам МДК; −практические работы по темам МДК; −выполнение рефератов, докладов; −участие в исследовательской, творческой работе; −оценка выполнения заданий для самостоятельной работы; −защита практических работ. Итоговый контроль: −комплексный экзамен по МДК 09.01. и МДК 09.02 −дифференцированный зачет по практике по профилю специальности; −квалификационный экзамен по профессиональному модулю.
ПК 9.2 Применять современные технологии и средства обеспечения информационной безопасности компьютерной сети	– правильность выбора методов и средств обеспечения информационной безопасности компьютерной сети в зависимости от рассматриваемого риска; – правильность описания метода защиты компьютерной сети, области его применения и особенностей реализации; – правильность применения методов и средств обеспечения информационной безопасности компьютерной сети; – полнота при перечислении выбранных методов и средств защиты компьютерной сети;	
ПК 5.4 Обеспечивать защиту программного обеспечения компьютерных систем	– точность в выборе методов и средств защиты программного обеспечения компьютерной системы в зависимости от его типа; – правильность описания метода защиты программного обеспечения компьютерной системы; – правильность применения методов и средств защиты программного обеспечения компьютерной системы; – полнота при перечислении выбранных методов и средств защиты программного обеспечения компьютерной системы.	

5.2 Контроль и оценка результатов освоения общих компетенций

Результаты (освоенные общие 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.	– точность в объяснениисоциальной значимости профессии; – проявление точности, аккуратности, внимательности при решении профессиональных задач; – демонстрация интереса к будущей профессии; – стремление к освоению профессиональных компетенций, знаний и умений (участие в предметных конкурсах, олимпиадах и др.);	– интерпретация результатов наблюдений за деятельностью студента в процессе освоения программы профессионального модуля; – активное участие в учебных, образовательных, воспитательных мероприятиях в рамках профессии; – достижение высоких результатов, стабильность результатов, портфолио достижений.
ОК 2 Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	– организация собственной деятельности в соответствии с поставленной целью; – определение и выбор способов (технологии) решения задачи в соответствии с заданными условиями и имеющимися ресурсами;	– интерпретация результатов наблюдений за деятельностью студента в процессе освоения программы профессионального модуля; – оценка за решение проблемно-ситуационных задач на практических занятиях; – устный и письменный экзамен; – положительные отзывы руководителей производственной практики от предприятий-баз практики.
ОК 3 Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.	– определение и выбор способа разрешения проблемы в соответствии с заданными критериями; – правильность проведения анализа ситуации по заданным критериям и определения рисков; – верность оценивания последствий принятых решений;	– интерпретация результатов наблюдений за деятельностью студента в процессе освоения программы профессионального модуля; – оценка за решение проблемно-ситуационных задач на практических занятиях; – устный и письменный экзамен; – положительные отзывы руководителей производственной практики от предприятий-баз практики.
ОК 4 Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.	– поиск и использование информации для эффективного выполнения профессиональных задач, профессионального и личностного развития;	

ОК 5 Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.	– корректное использование информационных источников для анализа, оценки и извлечения информационных данных, необходимых для решения профессиональных задач; – владение приёмами работы с компьютером, электронной почтой, Интернетом, активное применение информационно-коммуникационных технологий в профессиональной деятельности.	– интерпретация результатов наблюдений за деятельностью студента в процессе освоения программы профессионального модуля; – выполнение рефератов, заданий для самостоятельной работы, курсовой работы (проекта); – выполнение исследовательской творческой работы.
ОК 6 Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.	– взаимодействие с обучающимися, преподавателями в ходе обучения; – эффективное взаимодействие и общение с коллегами и руководством; – положительные отзывы с производственной практики.	– интерпретация результатов наблюдений за деятельностью студента в процессе освоения программы профессионального модуля; – участие в ролевых (деловых) играх и тренингах; – выполнение заданий учебной и производственной практики.
ОК 7 Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.	– ответственное отношение к результатам выполнения профессиональных обязанностей членами команды; – проведение самоанализа и коррекции результатов собственной работы;	
ОК 8 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, планировать повышение квалификации.	– владение механизмом целеполагания, планирования, организации, анализа, рефлексии, самооценки успешности собственной деятельности и коррекции результатов в области образовательной деятельности; – владение способами физического, духовного и интеллектуального саморазвития, эмоциональнойсаморегуляции и самоподдержки;	– интерпретация результатов наблюдений за деятельностью студента в процессе освоения программы профессионального модуля; – участие в ролевых (деловых) играх и тренингах; - выполнение рефератов, заданий для самостоятельной работы, курсовой работы (проекта); – выполнение исследовательской творческой работы; – выполнение заданий учебной и производственной практики.
ОК 9 Быть готовым к смене технологий в профессиональной деятельности.	– проявление интереса к инновациям в области профессиональной деятельности;	