****

**рабочая ПРОГРАММа**

ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

**ПМ.03При­ме­не­ние ин­же­нер­но-тех­ни­че­ских средств
обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти**

специальность**090305 Информационная безопасность автоматизированных систем**

Москва

2016

РАССМОТРЕНАУТВЕРЖДАЮ

Предметной (цикловой) Заместитель директора по ОУП

комиссией ОПД И ПМ специальности

090305

Протокол №\_\_1\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_И.Г.Бозрова

от «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2016г. «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2016г.

Председатель предметной (цикло-

вой) комиссии

\_\_\_\_\_\_\_\_\_ А.А.Юмаева

Разработчики:

Чагмавели Наталия Владимировна, преподаватель ГБПОУ КС № 54

Сверчков Евгений Евгеньевич, преподаватель ГБПОУ КС № 54

Бастрыкин К.М.,преподаватель ГБПОУ КС № 54

# **СОДЕРЖАНИЕ**

|  |
| --- |
| 1.Паспорт рабочей программы профессионального модуля.............….................4 |
| 2.Результаты освоения профессионального модуля..................…………………..6 |
| 3.Структура и содержание профессионального модуля ..........................................7 |
| 4.Условия реализации рабочей программы профессионального модуля.............19 |
| 5. Контроль и оценка результатов освоения профессионального модуля(вида профессиональной деятельности)…………........................…...…..………25 |

**1. паспорт рабочей ПРОГРАММЫ**

 **ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**1.1. Область применения программы**

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 090305 Информационная безопасность автоматизированных систем в части освоения основного вида профессиональной деятельности **При­ме­не­ние ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти** и соответствующих профессиональных компетенций (ПК):

ПК 3.1. При­ме­нять ин­же­нер­но-тех­ни­че­ские сред­ст­ва обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти.

ПК 3.2. Уча­ст­во­вать в экс­плуа­та­ции ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, уст­ра­не­нии от­ка­зов и вос­ста­нов­ле­нии ра­бо­то­спо­соб­но­сти.

ПК 3.3. Уча­ст­во­вать в мо­ни­то­рин­ге эф­фек­тив­но­сти при­ме­няе­мых ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной
безо­пас­но­сти.

ПК 3.4. Ре­шать ча­ст­ные тех­ни­че­ские за­да­чи, воз­ни­каю­щие
при проведении всех видов плановых и внеплановых контрольных проверок, при ат­те­ста­ции объ­ек­тов, по­ме­ще­ний, технических средств.

ПК 3.5. При­ме­нять нор­ма­тив­ные пра­во­вые ак­ты, нор­ма­тив­но-
ме­то­ди­че­ские до­ку­мен­ты по обес­пе­че­нию ин­фор­ма­ци­он­ной
безо­пас­но­сти ин­же­нер­но-тех­ни­че­ски­ми сред­ст­ва­ми.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании по повышению квалификации и переподготовки кадров в информатики и вычислительной техники при наличии среднего (полного) общего образования.

*Опыт работы* не требуется.

**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:**

* выявлениятех­ни­че­ских ка­на­лов утеч­ки
ин­фор­ма­ции;
* использования основных ме­то­дов и сред­ст­в ин­же­нер­но-тех­ни­че­ской за­щи­ты ин­фор­ма­ции;
* ди­аг­но­сти­ки, уст­ра­не­ния от­ка­зов и вос­ста­нов­ле­ния ра­бо­то­спо­соб­но­сти ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти;
* участия в мо­ни­то­рин­ге эф­фек­тив­но­сти ин­же­нер­но-
тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти;
* ре­ше­ния ча­ст­ных тех­ни­че­ских за­дач, воз­ни­каю­щих при ат­те­ста­ции объ­ек­тов, по­ме­ще­ний, тех­ни­че­ских средств;

**уметь:**

* при­ме­нять тех­ни­че­ские сред­ст­ва защиты информации;
* использовать средства ох­ра­ны и безо­пас­но­сти, ин­же­нер­ной за­щи­ты и тех­ни­че­ской ох­ра­ны объ­ек­тов, сис­тем ви­део­наб­лю­де­ния;
* использовать средства за­щи­ты ин­фор­ма­ции от несанкционированного съёма и утеч­ки по тех­ни­че­ским ка­на­лам;
* при­ме­нять нор­ма­тив­ные пра­во­вые ак­ты, нор­ма­тив­ные ме­то­ди­че­ские до­ку­мен­ты по обес­пе­че­нию ин­фор­ма­ци­он­ной безо­пас­но­сти тех­ни­че­ски­ми сред­ст­ва­ми;

**знать:**

* физику воз­ник­но­ве­ния технических каналов утеч­ки ин­фор­ма­ции, спо­со­бы их вы­яв­ле­ния и ме­то­ды оцен­ки опас­но­сти, клас­си­фи­ка­цию су­ще­ст­вую­щих фи­зи­че­ских по­лей и тех­ни­че­ских ка­на­лов утеч­ки ин­фор­ма­ции;
* но­менк­ла­ту­ру и ха­рак­те­ри­сти­ки ап­па­ра­ту­ры,
ис­поль­зуе­мой для съе­ма, пе­ре­хва­та и ана­ли­за
сиг­на­лов в тех­ни­че­ских ка­на­лах утеч­ки ин­фор­ма­ции;
* основные ме­то­ды и сред­ст­ва технической за­щи­ты ин­фор­ма­ции, но­менк­ла­ту­ру при­ме­няе­мых средств за­щи­ты ин­фор­ма­ции от несанкционированного съёма и утеч­ки по тех­ни­че­ским ка­на­лам;
* но­менк­ла­ту­ру при­ме­няе­мых средств ох­ра­ны и безо­пас­но­сти, ин­же­нер­ной за­щи­ты и тех­ни­че­ской ох­ра­ны объ­ек­тов, сис­тем ви­део­наб­лю­де­ния

**1.3Рекомендуемое количество часов**

**на освоение программы профессионального модуля:**

Всего – **1116**часов в том числе:

максимальной учебной нагрузки обучающегося – **864**часов, включая:

 - обязательной аудиторной учебной нагрузки обучающегося –**576**часов;

 - самостоятельной работы обучающегося –**288**часов;

 - учебной и производственной практики – **252** часа.

# **2. результаты освоения ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

Результатом освоения программы профессионального модуля является овладение обучающимися ВПД **Применение инженерно-технических средств обеспечения информационной безопасности**, в том числе профессиональными и общими компетенциями:

|  |  |
| --- | --- |
| **Код** | **Наименование результата обучения** |
| ПК 3.1. | При­ме­нять ин­же­нер­но-тех­ни­че­ские сред­ст­ва обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти. |
| ПК 3.2.  | Уча­ст­во­вать в экс­плуа­та­ции ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, уст­ра­не­нии от­ка­зов и вос­ста­нов­ле­нии ра­бо­то­спо­соб­но­сти. |
| ПК 3.3.  | Уча­ст­во­вать в мо­ни­то­рин­ге эф­фек­тив­но­сти при­ме­няе­мых ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти. |
| ПК 3.4.  | Ре­шать ча­ст­ные тех­ни­че­ские за­да­чи, воз­ни­каю­щие при проведении всех видов плановых и внеплановых контрольных проверок, при ат­те­ста­ции объ­ек­тов, по­ме­ще­ний, технических средств. |
| ПК 3.5.  | При­ме­нять нор­ма­тив­ные пра­во­вые ак­ты, нор­ма­тив­но-ме­то­ди­че­ские до­ку­мен­ты по обес­пе­че­нию ин­фор­ма­ци­он­ной безо­пас­но­сти ин­же­нер­но-тех­ни­че­ски­ми сред­ст­ва­ми. |
| ОК 1.  | Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности. |
| 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 их 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, осознанно планировать повышение квалификации. |
| ОК 9.  | Быть готовым к смене технологий в профессиональной деятельности. |
| ОК 10.  | Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей). |
|  |  |
| ОК 11. | Формулировать задачи логического характера и применять средства математической логики для их решения. |
| ОК 12.  | Владеть основными методами и средствами разработки программного обеспечения. |
| ОК 13. | Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах. |

**3.СТРУКТУРА и содержание профессионального модуля**

**3.1. Тематический план профессионального модуля**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Кодыпрофессиональныхкомпетенций** | **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,** часов | **Учебная,**часов | ***Производственная,****часов**(если предусмотрена рассредоточенная практика)* |
| **Всего,**часов | **в т.ч. лабораторные работы и практические занятия,**часов | **в т.ч. курсовая работа (проект),** часов | ***Всего, часов*** | ***в т.ч. курсовая работа******(проект), часов*** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | ***10*** |
| **ПК 3.1 – 3.5** | **Раздел 1.****Применение инженерно-технических средств обеспечения информационной безопасности** | **474** | **316** | 170 | - | **158** | - |  |  |
| **ПК 3.1 – 3.5**  | **Раздел 2.Ремонт и техническое обслуживание сетевого оборудования** | **264** | **176** | 84 |  | **88** |  |  |  |
| **ПК 3.1 – 3.5**  | **Раздел 3.Организация и защита беспроводных систем передачи информации** | **126** | **84** | 36 |  | **42** |  |  |  |
|  | **Учебная практика,** часов |  **72** |  |  |  |  |  | **72** |  |
|  | **Производственная практика (по профилю специальности),**часов | **180** |  |  |  |  |  |  | **180** |
|  ***Всего:*** | **1116** | **576** | **290** |  **-** | **288** | **-** |  **72** | **180** |

**3.2. Содержание обучения по профессиональному модулю (ПМ)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем** | **Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)** *(если предусмотрены)* | **Объем часов** | **Уровень освоения** |
| **1** | **2** | **3** | **4** |
| **Раздел 1.Применение инженерно-технических средств обеспечения информационной безопасности**  |  | **474** |  |
| **Введение** | Цели и задачи профессионального модуля. Структура профессионального модуля. Последовательность освоения профессиональных компетенций по модулю. Требования к уровню знаний и умений. | **2** | 1 |
| **МДК 03.01. Применение инженерно-технических средств обеспечения информационной безопасности** |  |  |  |
| **Тема 1.1. Информация и каналы утечки информации**  | **Содержание** | **30** | 3 |
|  | 1 | Понятие информации, защиты информации,информационной системы, безопасности автоматизированных систем обработки информации. |
| 2 | Цель защиты информации.  |
| 3 | Базовые свойства информации: конфиденциальность, целостность, доступность. |
| 4 | Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя. |
| 5 | Причины несанкционированного доступа к информации |
| 6 | Последствия несанкционированного доступа к информации. |
| 7 | Понятие угрозы, классификация угроз. |
| 8 | Понятие уязвимости, атаки на компьютерную систему. Понятие риска. |
| 9 |  Задача специалиста по информационной безопасности. |
| 10 | Виды утечки информации. Понятие канала утечки информации, основные каналы утечки информации и пути их возникновения. Классификация злоумышленников;Акустические каналы утечки информации; |
| 11 | Физика воз­ник­но­ве­ния технических каналов утеч­ки информации; |
| 12 | Фи­зи­че­ские по­ля и их возникновение ; |
| 13 | Классификация технических каналов утечки информации; |
| 14 | Основные ме­то­ды и сред­ст­ваин­же­нер­но-тех­ни­че­ской за­щи­ты ин­фор­ма­ции; |
| 15 | Программные способы защиты информации  |
|  | **Лабораторные работы**  | **26** |  |
| 1 |  Виды информации и основные методы ее защиты  |
| 2 |  Виды угроз информационной̆ безопасности Российской̆ Федерации.  |
| 3 | Источники угроз информационной̆ безопасности Российской̆ Федерации.  |
| 4 | Анализ информационной̆ инфраструктуры государства.  |
| 5 | Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации.  |
| 6 | Виды, каналы утечки и искажения информации  |
| 7 | Технические средства и методы защиты информации.  |
| 8 | Программно-аппаратные средства обеспечения информационной̆ безопасности.  |
| 9 | Испытания программных средств защиты.  |
| 10 | Защита от утечек по каналу ПЭМИН, по акустическому и виброаккустическому каналам. (4 часа) |
|  | 11 | Классификация программ по защите информации |  |
|  | 12 | Создание зашифрованного канала передачи данных  |  |
| **Тема 1.2.** **Ин­же­нер­но-тех­ни­че­ские средства защиты объектов информации**  | 1 | Подсистемы разграничения доступа к ресурсам.  | **38** | 3 |
| 2 | Цели применения криптографических преобразований, электронно-цифровой подписи.  |
| 3 | Аудит безопасности, резервирование ресурсов и компонентов автоматизированной системы.  |
| 4 | Типы аппаратуры в тех­ни­че­ских ка­на­лах утеч­ки ин­фор­ма­цииКлассификация ин­же­нер­но-тех­ни­че­ские средствКейс «ТЕНЬ» |
| 5 | Устройство для быстрого уничтожения информации на жесткихмагнитных дисках «СТЕК-Н» |
| 6 | Устройства идентификации iButton. История развития, внешний вид и структура электронного ключа iButton. Области применения, принципы конструкции iButton. |
| 7 | Бесконтактные радиочастотные карты prоximity. Внешний вид и принцип работы карт, пассивные и активные карты. |
| 8 | Пластиковые карты. Внешний вид и классификация пластиковых карт: карты со штрих кодом, карты с магнитной полосой, карты-счетчики |
| 9 | Карты с памятью, карты с микропроцессором. |
| 10 | Понятие и примеры биометрических характеристик человека |
| 11 | Особенность применения биометрических систем идентификации и аутентификации личности по сравнению с другими классами систем идентификации и аутентификации |
| 12 | Коэффициент ошибочных отказов и ошибочных подтверждений,  |
| 13 | Архитектура биометрических систем аутентификации, обучение биометрических систем |
| 14 | Системы перехвата и анализа сигналов  |
| 15 | Ха­рак­те­ри­сти­ки ап­па­ра­ту­ры в тех­ни­че­ских ка­на­лах утеч­ки ин­фор­ма­ции |
| 16 | Ра­бо­то­спо­соб­но­сть ин­же­нер­но-тех­ни­че­ских средств обеспечения информационной безопасности  |
| 17 | Причины отказов работоспособности  |
| 18 | Классификация проблем инженерно-технических средств обеспечения информационной безопасности  |
| 19 | Уст­ра­не­ния от­ка­зов и вос­ста­нов­ле­ния работоспособности ин­же­нер­но-тех­ни­че­ских средств обеспечения информационной безопасности |
|  **Лабораторные работы** | **44** |  |
| 1 | Сетевое сканирование  |
| 2 | Анализ трафика и сбор критичной информации программами пассивного анализа  |
| 3 | Дистанционное управление компьютером. |
| 4 | Обнаружение уязвимостей по сигнатурам  |
| 5 | Сетевые помехоподавляющие фильтры |
|  6 | Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф»  |
| 7 | Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор»  |
| 8 | Аудит комплексной защиты информации предприятия  |
| 9 | Технические средства защиты информации в телефонных линиях |
| 10 | Технические средства обнаружения, локализации средств негласного получения информации. |
| 11 | Нейтрализации радиоизлучающих специальных технических помех. |
| 12 | Контроль эффективности защиты речевой информации с помощью программно-аппаратного комплекса «СПРУТ- МИНИ» |
| 13 | Поиск и измерение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса«НАВИГАТОР-П3Г».(4 часа) |
| 14 | Акустические и виброакустические каналы утечки |
| 15 | Побочные эми от средств обработки информации |
| 16 | Исследование оптоэлектронного канала утечки информации |
| 17 | Технические средства защиты от утечек информации по проводным линиям |
| 18 | Идентификация с помощью биометрических устройств  |
| 19 | Применение активных и пассивный пластиковых карт  |
| 20 | Применение парольных систем различного типа  |
| **Тема 1.3.** **Ме­то­ды и сред­ст­ва за­щи­ты ин­фор­ма­ции** | 1 | Концепция и методы инженерно-технической̆ защиты информации; | **42** | 2 |
| 2 | Экранирование электромагнитных волн ;Экранированные помещения; |
| 3 | Безопасность оптоволоконных кабельных систем. |
| 4 | Заземление технических средств и подавление информационных сигналов в цепях заземления; |
| 5 | Фильтрация информационных сигналов, основные сведения о помехоподавляющих фильтрах; |
| 6 | Выбор типа фильтра; Пространственное и линейное зашумление. |
| 7 | Устройства контроля и защиты слаботочных линий и сети |
| 8 | Особенности слаботочных линий и сетей̆ как каналов утечки информации ; |
| 9 | Рекомендуемые схемы подключения анализаторов к электросиловым и телефонным линиям в здании |
| 10 | Устройства контроля и защиты проводных линий от утечки информации ; |
| 11 | Скрытие речевой информации в телефонных системах с использованием криптографических методов ; |
| 12 | Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах ; |
| 13 | SecretNet 5.0; |
| 14 | Электронный замок «СОБОЛЬ»; USB-ключ |
| 15 | Системы шифрования информации; |
| 16 | Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах. |
| 17 | Безопасность в сети. Сервисы. NFS (NetworkFileSystem) |
| 18 | Усиление базовой безопасности ОС Linux. |
| 19 | Понятие криптоанализа, криптоаналитической атаки. |
| 20 | Встроенные средства защиты ОС семейства Unix. Защитные механизмы, реализованные в Linux OS.LinuxSecurityModules (LSM), безопасность ядра Linux |
| 21 | Требования к шифрам, используемым для криптографической защиты информации. |
|  **Лабораторные работы** | **70** |  |
| 1 | Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладныхустройств в защищаемом помещении (4 часа) |
| 2 | Обнаружение сигналов линейных и сетевыхЗакладок |
| 3 | Обнаружение оптических сигналов передатчиков ик-диапазона |
| 4 | Программирование арифметических алгоритмов |
| 5 | Программирование алгебраических алгоритмов |
| 6 | Защита от закладок при разработке программ |
| 7 | Программирование алгоритмов криптосистем с открытом ключом |
| 8 | Профилактика заражения вирусами компьютерных систем |
| 9 | Биометрическая аутентификация пользователя по клавиатурному подчерку» |
| 10 | «Элементы криптоанализа.Оценка частотности символов в тексте» |
| 11 | Шифрованиеметодамиперестановки. |
| 12 | Шифрованиеметодомзамены |
| 13 | Шифрованиеметодомгаммирования. |
| 14 | Методы криптографической защиты информации.Простейшие алгоритмы шифрования |
| 15 | Шифр многоалфавитной замены — шифрование методом Вернама.  |
| 16 | Зашифровать и расшифровать выданное сообщение с помощью алгоритма шифрования RSA. |
| 17 | Методы и алгоритмы стеганографического сокрытия данных |
| 18 | Оценка уязвимости коммутируемого доступа |
| 19 | Произвести защиту вымышленного помещения (8 часов ) |
| 20 | Программно-аппаратный комплекс «спрут-7»  |
| 21 | Оценка защищенности ограждающихКонструкций помещения от утечки информации (6 часа ) |
| 22 | Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласногополучения информации, использующих силовые линии сети переменного тока и линии систем охранной (пожарной̆) сигнализации |
| 23 | Анализ систем видеонаблюдения  |
| 24 | Анализ систем защиты от прослушивания  |
| 25 | Скрытые функции диктофоны  |
| 26 | **«**Построение зависимости состояния защищенности от уровня экономического развития организации»(4часа ) |
| 27 | **«**Изучение международных стандартов во ИБ»(4 часа ) |
| **Тема 1.4. Ин­же­нер­ная и тех­ни­че­ская защита ох­ра­ны объ­ек­тов** | 1 | Категории объектов защиты; Особенности задач охраны различных типов объектов; (6часа ) | **34** | 2 |
| 2 | Общие принципы обеспечения безопасности объектов; |
| 3 | Система охранно-тревожной сигнализации; |
| 4 | Система контроля и управления доступом; Телевизионные системы; Система пожарной сигнализации;(4 часа ) |
| 5 | Периметровая охрана. Но­менк­ла­ту­ру при­ме­няе­мых средств ох­ра­ны и безо­пас­но­сти;(4 часа) |
| 6 | Системы видеонаблюдения |
| 7 | Технические каналы утечки видовой информации; Способы скрытого видеонаблюдения и съемки;  |
| 8 | Общие сведения. Мероприятия по выявлению и оценке свойств каналов утечки информации; ; |  |
| 9 | Специальные проверки; Специальные обследования; Специальные исследования;(4 часа ) |  |
| 10 | Специальные исследования акустических и виброакустических каналов ; |  |
| 11 | Специальные исследования акустоэлектрических преобразований; |  |
| 12 | Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок |  |
| **Лабораторные работы**  | **30** | 3 |
| 1 | Требования к средствам обеспечения безопасности. |  |
| 2 | **«**Планирование безопасности организации».(10 часов ) |  |
| 3 | **«**Изучение основных направлений деятельности СУИБ» |  |
| 4 | **«**Взаимодействие отдела обеспечения безопасности информации с другими подразделениями»**.** |  |
| 5 | «Изучение этапов разработки КСЗИ» |  |
| 6 | **«**Построение зависимости вида защищаемой информации от формы собственности предприятия» |  |
| 7 | «Конструктивные особенности организации, как фактор, влияющий на КСЗИ» |  |
| 8 | «Качественные показатели ресурс обеспечения, как факторы, влияющие на КСЗИ» |  |
| 9 | Степень автоматизации основных процедур обработки защищаемой информации. |  |
| 10 | Виды защищаемой информации на предприятии.(4 часа) |  |
|  |  |  |
| **Самостоятельная работа обучающегося при изучении раздела**  | 1.1 | Систематическая проработка конспектов занятий, учебной и специальной литературы. | **158** |  |
| 1.2 | Подготовка реферата по теме «идентификации и аутентификации " |
| 1.3 | Подготовка доклада по теме " Парольные системы " |
| 1.4 | Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. |
| 1,5 |  Презентация на тему «Программно-аппаратный комплекс «спрут-7» |
| 1,6 | Презентация на тему «Каналы утечки информации» |
| 1,7 | Подготовка презентации по теме " Прослушивание помещений " |
| 1,8 | Подготовка доклада на тему «Cетевое оборудование для обеспечения информационной безопасности » |
| 1,9 | Подготовка доклада на тему « Биометрические устройства для обеспечния безопасности» |
| 1,10 | Подготовить доклад на тему "Электронный замок «СОБОЛЬ " |
| 1,11 | Исследование Сетевых протоколов для безопасности системы (сравнительная таблица) |
| 1,12 | Подготовить презентацию на тему “ оптические сигналы передатчиков ” |
| 1,13 | Доклад на тему " Устройства идентификации iButton " |
| 1,14 | Правила проведения аттестации объектов (доклад) |
| 1,15 | Изучение технических устройств обеспечения защиты информации (сравнительная таблица) |
| 1,16 | Доклад на тему " Тестовые испытания программных средств защиты." |
| 1,17 | Произвести исследование типов вирусов (веб-квест) |
| **Раздел 2. Ремонт и техническое обслуживание сетевого оборудования** |  |  |  |  |
| **МДК 03.02 Ремонт и техническое обслуживание сетевого оборудования** |  |  | **264** |  |
| **Тема 2.1 Сетевые технологии** |  | **Содержание** | **24** | 2 |
| 1 | Локальные вычислительные сети |
| 2 | Сравнение узкополосных и широкополосных сетей |
| 3 | Сравнение коммутации пакетов и коммутации каналов |
| 4 | Сети и сетевые комплексы |
| 5 | Кабели и топологии |
| 6 | Управление доступом к среде передачи данных |
| 7 | Повторители и мосты |
| 8 | Коммутаторы и маршрутизаторы |
| 9 | Глобальные сети |
| 10 | Протоколы и стандарты |
| 11 | Клиенты и серверы |
| 12 | Операционные системы и приложения |
| **Тема 2.2 Сетевое аппаратное обеспечение** | **Содержание** | **32** | 2 |
| 1 | Платы сетевых адаптеров |
| 2 | Дополнительные возможности сетевых адаптеров |
| 3 | Полный дуплекс |
| 4 | Управление шиной |
| 5 | Параллельное выполнение задач |
| 6 | Дистанционное включение |
| 7 | Протокол  |
| 8 | Скорость передачи |
| 9 | Сетевой интерфейс  |
| 10 | Интерфейс шины |
| 11 | Требования к аппаратным ресурсам |
| 12 | Требования к электропитанию |
| 13 | Сетевые адаптеры для серверов |
| 14 | Сетевые адаптеры для рабочих станций |
| 15 | Драйверы сетевых адаптеров |
| 16 | Зачет |
| **Практические занятия** | **56** |  |
| 1 | Обжим витой пары по варианту А |
| 2 | Обжим витой пары по варианту В |
| 3 | Изучение сигналов физического уровня модели OSI |
| 4 | Изучение адресаций |
| 5 | Реализация управления доступом |
| 6 | Индикатор протоколов |
| 7 | Выявление ошибок канального уровня |
| 8 | Настройка маршрутизации |
| 9 | Фрагментация  |
| 10 | Изучение функций протоколов транспортного уровня |
| 11 | Сеансовый уровень. Управление диалогами. |
| 12 | Сеансовый уровень. Разделение диалогов. |
| 13 | Исправление ошибок представительского уровня. |
| 14 | Исправление ошибок прикладного уровня. |
| **Тема 2.3 Прокладка сетевого кабеля** | **Содержание** | **36** | 3 |
|  | 1 | Свойства кабеля |
| 2 | Стандарты кабельных систем |
| 3 | Стандарты протоколов канального уровня |
| 4 | Толстый кабель Ethernet |
| 5 | Тонкий кабель Ethernet |
| 6 | Технология ARCNET |
| 7 | Кабельное телевидение |
| 8 | Кабели на основе витой пары |
| 9 | Неэкранированная витая пара |
| 10 | Схема расположения контактов коннекторов |
| 11 | Оптоволоконный кабель |
| 12 | Строение оптоволоконного кабеля |
| 13 | Коннекторы для оптоволоконного кабеля |
| 14 | Прокладка кабеля |
| 15 | Монтаж оборудования |
| 16 | Тестирование соединений |
| 17 | Соединение компьютеров |
| 18 | Итог  |
| **Практические занятия** | **28** |  |
| 15 | Исследование повторителей |
| 16 | Исследование пассивных конденсаторов |
| 17 | Исследование мостов |
| 18 | Исследование коммутаторов |
| 19 | Исследование маршрутизаторов |
| 20 | Исследование выделенных линий |
| 21 | Исследование служб коммутации пакетов |
| **Самостоятельная работа обучающегося при изучении раздела**  |  | **88** |  |
| 2.1 | Уровни модели OSI (презентация) |
| 2.2 | Скорость передачи (конспект) |
| 2.3 | Сетевой интерфейс (конспект) |
| 2.4 | Сетевые адаптеры для серверов (конспект) |
| 2.5 | Сетевые адаптеры для рабочих станций (конспект) |
| 2.6 | Коннекторы (презентация) |
| 2.8 | Разновидности сетей (презентация) |
| 2.9 | Оптоволоконный кабель (презентация) |
| 2.10 | Составление тестов по изученному материалу |
| 2.11 | Техническое обслуживание сетевого оборудования (презентация) |
| 2.12 | Виды ремонта сетевого оборудования(реферат) |
| 2.13 | Подготовка к практическим занятиям. |
|  |  |
| **Раздел 3.Организация и защита беспроводных систем передачи информации** |  | **126** |  |
| **МДК 03.03 Организация и защита беспроводных систем передачи информации** |  |  |  |
| **Тема 3.1. Организационная структура системы обеспечения безопасности передачи информации.** | **Содержание** | **6** | 2 |
| 1 | Основы беспроводных сетей |
| 2 | Понятие технологии обеспечения безопасности передачи информации. |
| 3 | Институт ответственных за обеспечение безопасности передачи информации. |
| **Тема 3.2. Обязанности пользователей и ответственных за обеспечение безопасности передачи информации.** | **Содержание** | **4** | 3 |
| 1 | Общие правила обеспечения безопасности передачи информации при работе сотрудников.Ответственность за нарушения. |
| 2 | Порядок работы с носителями ключевой информации. |
| **Практические занятия** | **4** |  |
| 1 | Установка прав доступа пользователей к объектам доступа |
| 2 | Регистрация пользователей и установка их уровней доступа |
| **Тема 3.3. Требования к защите передачи информации и категорирование ресурсов.** | **Содержание** | **6** | 3 |
| 1 | Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. |
| 2 | Категорирование защищаемых ресурсов. |
| 3 | Взаимодействие подразделений на всех этапах передачи информации  |
| **Практические занятия** | **12** |  |
| 3 | Системный подход к защите информации |
| 4 | Моделирование объекта защиты |
| 5 | Подготовка рекомендаций по разработке мер защиты |
| 6 | Проведение информационных обследований защищаемых ресурсов |
| 7 | Документирование результатов обследования защищаемых ресурсов |
| 8 | Анализа защищённости беспроводных систем передачи информации |
| **Тема 3.4. Планы защиты и планы обеспечения непрерывной работы и восстановления беспроводных систем передачи информации.** | **Содержание** | **8** | 2 |
| 1 | Корректная настройка устройств |
| 2 | Отслеживание ложных узлов |
| 3 | Средства обеспечения непрерывной работы.  |
| 4 | Обязанности и действия персонала по обеспечению непрерывной работы. |
| **Практические занятия** | **6** |  |
| 9 | Восстановление беспроводных систем передачи информации. |
| 10 | Администрирование подсистем защиты передачи информации |
| 11 | Описать процесс защиты беспроводной сети |
| **Тема 3.5 Концепция безопасности информационных технологий предприятия.** | **Содержание** | **2** | 2 |
| 1 | Назначение и статус документа.Вопросы, которые должны быть отражены в Концепции. |
| **Практические занятия** | **4** |  |
| 12 | Разработка должностных инструкцийадминистратора безопасности системы защиты беспроводной сети. |
| 13 | Разработка нормативно-методических документов, позволяющих регламентировать эксплуатацию и сопровождение комплекса защиты беспроводной сети. |
| **Тема 3.6 Обнаружение и устранение уязвимостей передачи информации.** | **Содержание** | **8** | 3 |
| 1 | Архитектура систем управления уязвимостями |
| 2 | Особенности сетевых агентов сканирования |
| 3 | Специализированный анализ защищенности |
| 4 | Обзор средств анализа защищенности |
| **Практические занятия** | **8** |  |
| 14 | Оценка эффективности технических средства обнаружения негласного получения информации |
| 15 | Оценка эффективности технических средств локализации и нейтрализации утечки информации |
| 16 | Оценка эффективности защиты информации от утечки через радиоприборы |
| 17 | Устранения уязвимостей беспроводной сети. |
| **Тема 3.7. Мониторинг событий безопасности.** | **Содержание** | **6** | 2 |
| 1 | Инфраструктура управления журналами событий. Категории журналов событий |
| 2 | Введение в технологию обнаружения атак |
| 3 | Классификация систем обнаружения атак |
| **Тема 3.8. Средства защиты беспроводных сетей** | **Содержание** | **8** | 2 |
| 1 | Веб-конфигурирование точки доступа |
| 2 | Алгоритм привязки RADIUS-сервера к беспроводной сети |
| 3 | MAC-аутентификация |
| 4 | Широковещательная передача SSID |
| **Практические занятия** | **2** |  |
| 18 | Разработка комплекса защиты беспроводной сети: |
| **Самостоятельная работа обучающегося при изучении раздела** |  |  | **42** |  |
| 3.1 | Защита личного компьютера от несанкционированного доступа (доклад) |
| 3.2 | Моделирование угроз информации (презентация) |
| 3.3 | Технические каналы утечки информации (конспект) |
| 3.4 | Обеспечение безопасности ИТ предприятия (презентация) |
| 3.5 | Обзор программных средств обнаружения и устранения уязвимостей при передаче информации (реферат) |
| 3.6 | Способы обнаружения атак (презентация) |
| 3.7 | Подготовка к практическим занятиям, оформление отчета по ПЗ и подготовка к их защите |
| **Учебная практика**  | **Виды работ:**Создание защищённого канала передачи данных Настройка идентификации пользователей в автоматизированной системе Тестирование пожарно- охранной сигнализацииОтслеживание журнала аудита Проверка системы на вирусы и несанкционированный доступ | **72** |  |
| **Производственная практика** | **Виды работ:**Выявлениетех­ни­че­ских ка­на­лов утеч­ки ин­фор­ма­ции;Использование основных ме­то­дов и сред­ст­в ин­же­нер­но-тех­ни­че­ской за­щи­ты ин­фор­ма­ции;Ди­аг­но­сти­ки, уст­ра­не­ния от­ка­зов и вос­ста­нов­ле­ние ра­бо­то­спо­соб­но­сти ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти; Участие в мо­ни­то­рин­ге эф­фек­тив­но­сти ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти;Ре­ше­ние ча­ст­ных тех­ни­че­ских за­дач, воз­ни­каю­щих при ат­те­ста­ции объ­ек­тов, по­ме­ще­ний, тех­ни­че­ских средств. | **180** |  |
| **Всего** | **1116** |  |

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 рабочей программы ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

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

Реализация программы модуля предполагает наличие учебного кабинета «Информационной безопасности»

**Оборудование учебного кабинета:**

-автоматизированные рабочие места по количеству обучающихся;

-автоматизированное рабочее место преподавателя;

-специализированная мебель;

-комплект нормативных документов;

-комплект учебно-методической литературы.

*Технические средства обучения:*

-проектор;

-экран;

-сканер;

-принтер;

-программное обеспечение общего и профессионального назначения.

**Оборудование лаборатории:**

-автоматизированные рабочие места по количеству обучающихся;

-автоматизированное рабочее место преподавателя;

-специализированная мебель;

-комплект нормативных документов;

-комплект учебно-методической литературы.

*Технические средства обучения:*

-проектор;

-экран;

-сканер;

-принтер;

-терминальные сервер;

-серверный шкаф со стойками;

-тонкие клиенты;

-комплект сетевого оборудования (сетевые адаптеры; повторители, сетевые коммутаторы, модули множественного доступа, концентраторы, мосты, маршрутизаторы, мосты-маршрутизаторы, шлюзы);

-соединительные патч-коды;

-программное обеспечение общего и профессионального назначения.

Реализация профессионального модуля предполагает обязательную производственную практику, которую можно проводить как концентрированно, т. е. После изучения МДК, так и рассредоточено.

# **4.2. Информационное обеспечение обучения**

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

**Основные источники:**

1. Блинов А.М., Информационная безопасность. – СПб.: ГУЭФ, 2013
2. Грибунин В.Г., ЧудовскийВ.В.Комплексная система защиты информации на предприятии – Спб.: «Академия», 2010.
3. Ватаманюк А. Инженерно-техническая защита информации: Учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности СПб.: Питер, 2010.
4. Торокин А.А.,Основы инженерно-технической защиты информации.- М.: 2013

**Дополнительные источники:**

1. Торокин А. А. Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел: Учебн. Пособие М.: Гелиос АРВ, 2005.
2. Романова Д.А.,Защита информации и конфиденциальные данные.-М.: Ника, 2009.

**Интернет-ресурсы:**

1 Журнал сетевых решений LAN [Электронный ресурс]. URL:[http://www.osp.ru/lan/#/home](http://www.osp.ru/lan/%23/home%20)

2 Журнал о компьютерных сетях и телекоммуникационных технологиях «Сети и системы связи» [Электронный ресурс].URL: <http://www.ccc.ru/>

3 <http://www.pandia.ru/>

# **4.3. Общие требования к организации образовательного процесса**

Освоению данного профессионального модуля предшествует освоение программ общепрофессиональных дисциплин:

ОП.01. Основы информационной безопасности

ОП.02. Технические средства информатизации

ОП.03. Организационно-правовое обеспечение информационной безопасности

ОП.04. Сети и системы передачи информации

ОП.05. Основы алгоритмизации и программирования

ОП.06. Электроника и схемотехника

ОП.07. Операционные системы

Производственная практика проводится концентрированно в организациях, направление деятельности которых соответствует профилю подготовки обучающихся. Предусматривается сдача зачета по производственной практике (по профилю специальности).

Освоение каждого междисциплинарного курса завершается экзаменом, а освоение программы профессионального модуля – проведением квалификационного экзамена.

# **4.4. Кадровое обеспечение образовательного процесса**

**Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарному курсу (курсам):** наличие высшего профессионального образования, соответствующего профилю модуля и специальности.

**Требования к квалификации педагогических кадров, осуществляющих руководство практикой:**

* **педагогический состав**: дипломированные специалисты – преподаватели междисциплинарных курсов

# **мастера:** наличие 5-6-го квалификационного разряда с обязательной стажировкой в профильных организациях не реже 1 раза в 3 года. Опыт деятельности в организациях соответствующей профессиональной сферы или должности системного администратора обязателен.

# **5. Контроль и оценка результатов**

# **освоения профессионального модуля**

|  |  |  |
| --- | --- | --- |
| **Результаты** **(освоенные профессиональные компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки**  |
| ПК 3.1. При­ме­нять ин­же­нер­но-тех­ни­че­ские сред­ст­ва обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти. | - обоснованность выбора инженерных, технических и организационных решений;- точность и грамотность оформления организационной и технической документации | Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы:- при выполнении и защите курсовой работы (проекта);- при выполнении работ на различных этапах производственной практики;- при проведении контрольных работ, зачетов,экзаменов по МДК. |
| ПК 3.2. Уча­ст­во­вать в экс­плуа­та­ции ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, уст­ра­не­нии от­ка­зов и вос­ста­нов­ле­нии ра­бо­то­спо­соб­но­сти | умение решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых конnрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.- умение осуществлять мероприятия по выявлению и оценке свойствканалов утечки информации | Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх);- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов,экзаменов по МДК. |
| ПК 3.3. Уча­ст­во­вать в мо­ни­то­рин­ге эф­фек­тив­но­сти при­ме­няе­мых ин­же­нер­но-тех­ни­че­ских средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти. | - точность и скорость диагностики нарушений эксплуатационных характеристик систем;-качествоанализа эксплуатационныхсвойств системы, исходя из ее служебного назначения;- качество рекомендаций по повышению эксплуатационных свойств системы;- проверка технического состояния системы;- умения проводить техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность | Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы:- на практических занятиях (при выполнении и защите лабораторных (практических) работ);- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов,экзаменов по МДК. |
| ПК 3.4. Ре­шать ча­ст­ные тех­ни­че­ские за­да­чи, воз­ни­каю­щие при проведении всех видов плановых и внеплановых контрольных проверок, при ат­те­ста­ции объ­ек­тов, по­ме­ще­ний, технических средств. | - умение решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.- умение осуществлять мероприятия по выявлению и оценке свойств каналов утечки информации | Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы:- на практических занятиях (при выполнении и защите лабораторных (практических) работ);- при выполнении работ на различных этапах производственной практики. |
| ПК 3.5. При­ме­нять нор­ма­тив­ные пра­во­вые ак­ты, нор­ма­тив­но-ме­то­ди­че­ские до­ку­мен­ты по обес­пе­че­нию ин­фор­ма­ци­он­ной безо­пас­но­сти ин­же­нер­но-тех­ни­че­ски­ми сред­ст­ва­ми. | точность и грамотность применения нормативных правовых актов, нормативно-методических документов по обеспечению информационной̆ безопасности инженерно-техническими средствами | Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы:- на практических занятиях (при выполнении и защите лабораторных (практических) работ), при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.)- при выполнении и защите курсовой работы (проекта)- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов,экзаменов по МДК |

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 общие компетенции)** | **Основные показатели оценки результата** | **Формы контроля и оценка** |
| ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес. | -участие в работе студенческих научных обществ;- выступления на научно-практических конференциях;- участие во внеурочной деятельности связанной с будущей профессией/специальностью (конкурсы профессионального мастерства, выставки и т.п.)- высокие показатели производственной деятельности | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. | - выбор и применение методов и способов решения профессиональных задач, оценка их эффективности и качества | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность | - анализ профессиональных ситуации;- решение стандартных и нестандартных профессиональных задач | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. | - эффективный поиск необходимой информации;- использование различных источников, включая электронные при изучении теоретического материала и прохождении различных этапов производственной практики  | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности. | * использование в учебной и профессиональной деятельности различных видов программного обеспечения, в том числе специального, при оформлении презентации всех видов работ
 | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. | взаимодействие:- с обучающимися при проведении деловых игр, выполнении коллективных заданий (проектов), - с преподавателями, мастерами в ходе обучения, - с потребителями и коллегами в ходе производственной практики | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК 7. Брать на себя ответственность заработу членов команды (подчиненных), за результат выполнения заданий. | - самоанализ и коррекция результатов собственной деятельности при выполнении коллективных заданий (проектов);- ответственность за результат выполнения заданий | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. | - планирование и качественное выполнение заданий для самостоятельной работы при изучении теоретического материала и прохождении различных этапов производственной практики;- определение этапов и содержания работы по реализации самообразования | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности. | - адаптация к изменяющимся условиям профессиональной деятельности;- проявление профессиональной маневренности при прохождении различных этапов производственной практики | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей). | Исполнение воинской обязанности, в том числе с применением полученных профессиональных знаний (для юношей) | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК11. Формулировать задачи логического характера и применять средства математической логики для их решения. | демонстрация способности формулировать задачи логического характера и применять для их решения средства математической логики | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК 12. Владеть основными методами и средствами разработки программного обеспечения. | демонстрация умения применять основные методы и средства разработки программного обеспечения | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
| ОК 13.. Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах. | демонстрация умения производить инсталляцию и настройку автоматизированных информационных систем, выполнять регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах автоматизированных информационных систем | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:- на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.);- при выполнении работ на различных этапах производственной практики;*-* при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю. |
|  |