**ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**УЧАСТИЕ В ПЛАНИРОВАНИИ И ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ОБЪЕКТА**

БАЗОВАЯ ПОДГОТОВКА

2014 г.

Программа профессионального модуля ***ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта*** разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) **10.02.01 Организация и технология защиты информации** по программе базовой подготовки.

Организация-разработчик: Областное государственное бюджетное профессиональное образовательное учреждение «Смоленская академия профессионального образования»

Разработчик:

Ромашкова И.А., преподаватель ОБГПОУ СмолАПО

Ефремова Ю. М., преподаватель ОБГПОУ СмолАПО

Утверждена Научно-методическим советом ОБГПОУ СмолАПО

Протокол № 1 от 05.09.2014 г.

Рассмотрена на заседании кафедры Информационных технологий

Протокол № 1 от 02.09.2014 г.

**СОДЕРЖАНИЕ**

[**1.** **ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** 4](#_Toc316050115)

[**2.** **РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** 7](#_Toc316050133)

[**3.** **СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** 9](#_Toc316050134)

[**4.** **УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** 18](#_Toc316050139)

[**5.** **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)** 21](#_Toc316050140)

# **ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

# **ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта**

**1.1. Область применения программы**

Программа профессионального модуля – является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.01 Организация и технология защиты информации базовой подготовки в части освоения вида профессиональной деятельности (ВПД): **Участие в планировании и организации работ по обеспечению защиты объекта** и соответствующих профессиональных компетенций (ПК):

* участвовать в сборе и обработке материалов для выработки оптимальных решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации;
* участвовать в разработке программ и методик организации защиты информации на объекте;
* осуществлять планирование и организацию выполнения мероприятий по защите информации;
* участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности;
* вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации;
* обеспечивать технику безопасности при проведении организационно-технических мероприятий;
* участвовать в организации и проведении проверок объектов информатизации, подлежащих защите;
* проводить контроль соблюдения персоналом требований режима защиты информации.
* участвовать в оценке качества защиты объекта.

Программа профессионального модуля может быть использована в дополнительном образовании по направлению подготовки 10.02.01 Организация и технология защиты информации (базовый уровень) и в профессиональной подготовке по профессиям:

27032 Техник по защите информации

27069 Техник по техническим средствам обучения

26965 Техник вычислительного (информационно-вычислительного) центра

230103.04 Наладчик аппаратного и программного обеспечения

**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:**

* использования физических средств защиты объекта;
* применения физических средств контроля доступа на объект;
* ведения текущей работы исполнителей с конфиденциальной информацией;
* участия в разработке, внедрении и сопровождении политики безопасности;

**уметь***:*

* организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;
* пользоваться аппаратурой систем контроля доступа;
* выделять зоны доступа по типу и степени конфиденциальности работ;
* определять порядок организации и проведения рабочих совещаний;
* использовать методы защиты информации в рекламной и выставочной деятельности;
* использовать критерии подбора и расстановки сотрудников подразделений защиты информации;
* организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;
* проводить инструктаж персонала по организации работы с конфиденциальной информацией;
* контролировать соблюдение персоналом требований режима защиты информации;
* разрабатывать политику безопасности организации;
* внедрять и сопровождать политику безопасности организации;

**знать***:*

* виды и способы охраны объекта;
* особенности охраны персонала организации;
* основные направления и методы организации режима и охраны объекта;
* разрешительную систему доступа к конфиденциальной информации;
* принципы действия аппаратуры систем контроля доступа;
* принципы построения и функционирования биометрических систем безопасности;
* требования и особенности оборудования режимных помещений;
* требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров;
* требования режима защиты информации при приеме в организации посетителей;
* организацию работы при осуществлении международного сотрудничества;
* требования режима защиты информации в процессе рекламной деятельности;
* требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати;
* задачи, функции и структуру подразделений защиты информации;
* принципы, методы и технологию управления подразделений защиты информации;
* методы проверки персонала по защите информации;
* процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией;
* порядок разработки политики безопасности организации;
* уровни детализации политики информационной безопасности;
* законодательные основы политики информационной безопасности.

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

всего – 606 часа, в том числе:

- максимальной учебной нагрузки обучающегося – 390 часов, включая:

- обязательной аудиторной учебной нагрузки обучающегося – 260 часа;

- самостоятельной работы обучающегося – 130 часов,

- учебной практики и практики по профилю специальности – 216 часа.

# **РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности **Участие в планировании и организации работ по обеспечению защиты объекта**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

|  |  |
| --- | --- |
| **Код** | **Наименование результата обучения** |
| ПК 1.1. | Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации. |
| ПК 1.2. | Участвовать в разработке программ и методик организации защиты информации на объекте. |
| ПК 1.3. | Осуществлять планирование и организацию выполнения мероприятий по защите информации. |
| ПК 1.4. | Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности. |
| ПК 1.5. | Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации. |
| ПК 1.6. | Обеспечивать технику безопасности при проведении организационно-технических мероприятий. |
| ПК 1.7. | Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите. |
| ПК 1.8. | Проводить контроль соблюдения персоналом требований режима защиты информации. |
| ПК 1.9. | Участвовать в оценке качества защиты объекта. |
| 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, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. |
| ОК 3 | Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. |
| ОК 4 | Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. |
| ОК 5 | Использовать информационно-коммуникационные технологии в профессиональной деятельности. |
| ОК 6 | Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. |
| ОК 7 | Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. |
| ОК 8 | Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| ОК 9 | Ориентироваться в условиях частой смены технологий в профессиональной деятельности. |
| ОК 10 | Применять математический аппарат для решения профессиональных задач. |
| ОК 11 | Оценивать значимость документов, применяемых в профессиональной деятельности. |
| ОК 12 | Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность. |

# **СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

* 1. **Тематический план профессионального модуля**

**ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 1.1 – ПК 1.3, ПК 1.8.,** **ПК 1.7.** | **Раздел 1 Обеспечение организации системы безопасности предприятия** | **96** | **64** | 28 | - | **32** | - | **36** | **-** |
| **ПК 1.1- ПК 1.3, ПК 1.5., ПК 1.7- ПК 1.9** | **Раздел 2**  **Организация работ подразделений защиты информации** | **120** | **80** | 32 | - | **40** | - | **-** | **-** |
| **ПК 1.1- ПК 1.3, ПК 1.5., ПК 1.7- ПК 1.9** | **Раздел 3**  **Организация работы персонала с конфиденциальной информацией** | **78** | **52** | 28 | - | **26** | - | **36** | **72** |
| **ПК 1.1- ПК 1.3, ПК 1.5., ПК 1.7- ПК 1.9** | **Раздел 4**  **Разработка внедрение и сопровождение политики безопасности** | **96** | **64** | 24 | 20 | **32** |  |  | **72** |
|  | **Производственная практика (по профилю специальности)**, часов |  |  | | | | | | **144** |
|  | **Всего:** | **390** | **260** | **112** | - | **130** | - | **72** | **144** |

**3.2. Содержание обучения по профессиональному модулю ПМ 01 «Участие в планировании и организации работ по обеспечению защиты объекта»**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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.01 Участие в планировании и организации работ по обеспечению защиты объекта** |  | | | | | **390** |  |
| **Раздел 1 ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта** |  | | | | | **96** |  |
| **МДК.01.01.** **Обеспечение организации системы безопасности предприятия** |  | | | | | **96** |
| Тема 1.1Введение. Место и роль системы безопасности в системе защиты предприятия | **Содержание** | | | | | **4** | 2 |
| 1 | | Необходимость и сущность системы безопасности | | |  |
| 2 | | Концепция безопасности фирмы | | |
| 3 | | Основные направления, принципы и условия организационной зашиты информации | | |
| 4 | | Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия | | |
| 5 | | Основные подходы и требования к организации системы защиты информации | | |
| Тема 1.2  Задачи и функции системы безопасности | **Содержание** | | | | | **16** | 2 |
| 1 | | Система безопасности фирмы. Правовые основы деятельности системы безопасности | | |  |
| 2 | | Положение о системе безопасности предприятия | | |
| 3 | | Задачи и функции службы безопасности | | |
| 4 | | Принципы и направления взаимодействия СБ с правоохранительными органами | | |
| 5 | | Управление безопасностью | | |
| 6 | | Основные виды угроз, классификация угроз, ущерб информационной безопасности предприятия | | |
| 7 | | Оценка уязвимостей системы безопасности | | |
| **Семинарские занятия** | | | | | **10** | 3 |
| **Практическая работа** | | | | | **6** | 2 |
| 1 | | Составление организационной структуры данной организации и выявление ее сферы деятельности. Создание описания виртуальной организации. | | |
| 2 | | Выявление бизнес-процессов организации. Составление необходимых документов. | | |
| Тема 1.3  Состав и структура системы безопасности | **Содержание** | | | | | **12** | 3 |
| 1 | | Состав и структура системы безопасности | | |  |
| 2 | | Направления защиты | | |
| 3 | | Средства и способы защиты | | |
| 4 | | Совет по безопасности предприятия | | |
| 5 | | Состав службы безопасности фирмы | | |
| 6 | | Штаты службы безопасности | | |
| 7 | | Руководитель службы безопасности | | |
| **Семинарские занятия** | | | | | **6** |
| **Практическая работа** | | | | | **8** |
| 1 | | Разработка структуры системы безопасности предприятия | | |
|  | 2 | | Подбор персонала и составление должностных инструкций | | |  |  |
| Тема 1.4  Построение политики безопасности предприятия | **Содержание** | | | | | **18** | 2 |
| 1 | | Основные цели планирования мероприятий по организационной защите информации на предприятии, | | |  |
| 2 | | Структура и основное содержание плана мероприятий по защите конфиденциальной информации | | |
| 3 | | Понятие политики безопасности | | |
| 4 | | Уровни политики безопасности предприятия | | |
| 5 | | Анализ рисков системы безопасности | | |
| 6 | | Стратегия защиты информационной безопасности. | | |
| 7 | | Ответственные и порядок контроля выполнения программы защиты | | |
| **Семинарские занятия** | | | | | 8 | 3 |
| **Практическая работа** | | | | | **10** | 3 |
| 1 | | Выявление рисков виртуального предприятия | | |
| 2 | | Построение модели угроз безопасности предприятия | | |
| 3 | | Разработка политики безопасности предприятия | | |
|  | 4 | | Построение модели нарушителя информационной безопасности | | |
| Тема 1.5  Подбор, расстановка и обучение сотрудников службы  безопасности | **Содержание** | | | | | **12** | 3 |
| 1 | | Кадровая политика безопасности | | |  |
| 2 | | Ведение досье на работников | | |
| 3 | | Методы получения, сбора и обработки информации для ведения досье | | |
| 4 | | Тестирование кандидатов | | |
| 5 | | Проверка персонала во время работы | | |
| 6 | | Обучение сотрудников службы безопасности | | |
| 7 | | Проведение служебного расследования по фактам имущественных преступлений | | |
| **Семинарские занятия** | | | | | 8 | 3 |
| **Практическая работа** | | | | | **4** | 3 |
| 1 | | Разработка типовых документов для функционирования службы безопасности | | |
| 2 | | Разработка документов, регулирующих обязанности лиц, допущенных к конфиденциальной информации | | |
| **Самостоятельная работа при изучении раздела ПМ 1**   1. Подготовка доклада. 2. Составление опорного конспекта. 3. Составление тезисов. 4. Работа с электронными информационными ресурсами и ресурсами Internet 5. Решение вариативных задач и упражнений. | | | | | | **32** |  |
| **Примерная тематика внеаудиторной самостоятельной работы**   1. Подготовка презентации по теме «Структура и штаты службы безопасности». 2. Составление терминологического словаря по модулю «Участие в планировании и организации работ по обеспечению защиты объекта». 3. Подготовка рефератов. 4. Чтение дополнительной литературы. 5. Ответы на контрольные вопросы. 6. Составление тестовых заданий по темам семинарских занятий. | | | | | |  |  |
| **Виды работ по учебной практике**   * Изучение средств контроля и ограничения доступа на объект * Выделение зон доступа по типу и степени конфиденциальности работ * Определение правил техники безопасности при проведении организационно-технических мероприятий информацией. * Разработка типовых документов для функционирования службы безопасности. | | | | | | **18** |  |
| **Раздел 2 ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта** |  | | | | | **120** |  |
| **МДК.01.02.** **Организация работ подразделений защиты информации** |  | | | | | **120** |  |
| Тема 1.1Введение. Необходимость и сущность служюы безопасности. Цели и задачи службы безопасности организации. | **Содержание** | | | | | **2** | 2 |
| 1 | | Основные понятия и определения | | |  |
| 2 | | Цели и задачи системы безопасности | | |
| 3 | | Концепция безопасности организации | | |
| Тема 1.2  Служба безопасности организации | **Содержание** | | | | | **20** | 3 |
| 1 | | Основное содержание деятельности службы информационной безопасности организации. | | |  |
| 2 | | Служба безопасности как самостоятельная организационная единица организации. | | |
| 3 | | Нештатные структуры службы безопасности. | | |
| 4 | | Характеристика подразделений службы безопасности и их функции | | |
| 5 | | Органы управления службой безопасности организации. | | |
| 6 | | Определение функций органов управления службой безопасности | | |
| 7 | | Основные составляющие обеспечения безопасности ресурсов коммерческой организации. | | |
| 8 | | Правила подбора персонала в службу безопасности | | |
| 9 | | Правила инструктажа сотрудников службы безопасности | | |
| 10 | | Организация реагирования на чрезвычайные ситуации (инциденты) | | |  |
| **Семинарские занятия** | | | | | **12** | 3 |
| **Практическая работа** | | | | | **8** | 3 |
| 1 | | Создание виртуальной службы безопасности организации | | |  |
| 2 | | Определение вида деятельности службы безопасности | | |
| 3 | | Определение необходимых структур и подразделений службы безопасности и их функций | | |
| 4 | | Подбор персонала в службу безопасности | | |
| Тема 1.3  Отдел режима и охраны службы безопасности | **Содержание** | | | | | **16** | 3 |
| 1 | | Организация режима и охраны | | |  |
| 2 | | Пропускные документы и их учет | | |
| 3 | | Охранная деятельность службы безопасности. | | |
| 4 | | Охрана финансовых средств | | |
| 5 | | Обеспечение безопасности персонала. | | |
| 6 | | Обеспечение охраны стационарных объектов | | |
| 7 | | Охрана с помощью технических средств | | |
| 8 | | Охрана путем выставления постов | | |
| 9 | | Комбинированная охрана | | |
| **Семинарские занятия** | | | | | **10** |
| **Практическая работа** | | | | | **6** |
| 1 | | Создание виртуального отдела режима и охраны службы безопасности. Определение функций каждого отдела режима и охраны службы безопасности | | |  | 3 |
| 2 | | Разработка должностных инструкций, положений, журналов учета, бланков отдела режима и охраны службы безопасности. | | |
| Тема 1.4  Отдел инженерно-технической безопасности | **Содержание** | | | | | **16** | 3 |
| 1 | | Организация инженерно-технической безопасности. | | |  |  |
| 2 | | Методы и способы инженерно-технической безопасности. | | |
| 3 | | Категорирование выделенных помещений | | |
| 4 | | Технический паспорт на защищаемое помещение | | |
| 5 | | Организационно-технические мероприятия инженерно-технической безопасности | | |
| **Семинарские занятия** | | | | | **8** |
| **Практическая работа** | | | | | **8** | 3 |
| 1 | | Создание виртуального отдела инженерно-технической безопасности | | |
| 2 | | Разработка организационных мероприятий инженерно-технической безопасности | | |
| 3 | | Разработка организационно-технических мероприятий инженерно-технической безопасности | | |
| 4 | | Разработка мероприятий по блокированию несанкционированного получения информации с помощью технических средств | | |
| Тема 1.5  Отдел информационно-аналитической деятельности. | **Содержание** | | | | | **12** | 2 |
| 1 | | Основные направления деятельности и функции группы информационно-аналитической деятельности | | |  |
| 2 | | Организация информационно-аналитической работы. | | |
|  | | Содержание и основные виды аналитических отчетов | | |
|  | | Классификация методов анализа информации | | |
| 3 | | Порядок оценки степени реальных конкурентных отношений. | | |
| **Семинарские занятия** | | | | | **6** | 3 |
| **Практическая работа** | | | | | **6** | 2 |
| 1 | | Создание виртуального отдела информационно-аналитической деятельности | | |  |
| 2 | | Определение вида деятельности информационно-аналитического отдела | | |
| 3 | | Выявление взаимодействия с другими информационными системами организации и внешними организациями | | |
| Тема 1.6  Отдел кадров и специальный отдел | **Содержание** | | | | | **8** | 3 |
| 1 | | Особенности работы отдела кадров | | |  | 3 |
| 2 | | Положение об отделе кадров, должностные инструкции | | |
| 3 | | Обеспечение безопасности конфиденциальной информации | | |
| 4 | | Обеспечение сохранности документов, дел и изданий | | |
| 5 | | Организация работы с кадрами | | |
| **Семинарские занятия** | | | | | **6** |
| **Практическая работа** | | | | | **2** |
| 1 | | Разработка должностных инструкций сотрудников службы защиты информации | | |  |
| Тема 1.7  Аудит безопасности организации | **Содержание** | | | | | **6** | 3 |
| 1 | | Особенности аудита безопасности | | |  | 3 |
| 2 | | Практика аудита информационной безопасности | | |
| 3 | | Оценка состояния защищенности предприятия | | |
| **Семинарские занятия** | | | | | **4** |
| **Практическая работа** | | | | | **2** |
| 1 | | Проведение аудита информационной безопасности виртуального предприятия | | |  |
| **Самостоятельная работа при изучении раздела ПМ 1**   * Подготовка доклада. * Составление опорного конспекта. * Составление тезисов. * Работа с электронными информационными ресурсами и ресурсами Internet * Решение вариативных задач и упражнений. | | | | | | **40** |  |
| **Примерная тематика внеаудиторной самостоятельной работы**   * Подготовка презентации при выполнении практических работ. * Составление терминологического словаря по модулю «Организация работ подразделений защиты информации». * Подготовка рефератов. * Чтение дополнительной литературы. * Ответы на контрольные вопросы. * Составление тестовых заданий по темам семинарских занятий. | | | | | |  |  |
| **Виды работ по учебной практике**   * Изучение правил подбора персонала в службу безопасности * Изучение видов пропускных документов * Изучение способов учета пропускных документов * Разработка должностных инструкций сотрудников службы защиты информации | | | | | | **18** |  |
| **Раздел 3 ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта** |  | | | | | **78** |  |
| **МДК.01.03.** **Организация работы персонала с конфиденциальной информацией** |  | | | | | **78** |  |
| Тема 1.1. Введение. Задачи курса. Нормативная документация. | **Содержание** | | | | | **4** | 2 |
| 1 | | Предмет, задачи и содержание курса | | |  |  |
| 2 | | Предпосылки и направления совершенствования технологии защиты и обработки конфиденциальных документов | | |
| 3 | | Назначение курса и его роль в подготовке специалистов по защите информации | | |
| 4 | | Основные нормативные правовые акты и методические документы по защите конфиденциальной информации | | |
|  | **Семинарские занятия** | | | | | **2** |
| **Практическая работа** | | | | | **2** |
| 1 | | | | Изучение нормативных правовых актов по защите информации |
| Тема 1.2. Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений | **Содержание** | | | | | **10** | 3 |
| 1 | | Отнесение сведений к различным видам конфиденциальной информации | | |  | 3 |
| 2 | | Отнесение сведений к коммерческой тайне | | |
| 3 | | Реквизиты носителей сведений | | |
| 4 | | Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну | | |
| 5 | | Отнесение сведений к государственной тайне | | |
| 6 | | Засекречивание сведений и их носителей | | |
| 7 | | Основания и порядок рассекречивания сведений и их носителей. Основания для рассекречивания. | | |
| **Семинарские занятия** | | | | | **4** | 3 |
| **Практическая работа** | | | | | **6** | 3 |
| 1 | | Создание виртуальной организации и определение ее сферы деятельности | | |
| 2 | | Составление списка документов, составляющих конфиденциальную информацию | | |
| 3 | | Составление списка сотрудников имеющих права доступа к конфиденциальной информации различных грифов секретности | | |
| 4 | | Разработка инструкции по обеспечению сохранности конфиденциальной информации на примере организации | | |
| Тема 1.3. Организация режима защиты информации | **Содержание** | | | | | **12** | 2 |
| 1 | | Организация режима защиты информации при приеме в организации посетителей | | |  |
| 2 | | Порядок допуска и доступа персонала и иных лиц к КИ | | |
| 3 | | Организационные требования к режимным помещениям | | |
| 4 | | Организационная защита информации в процессе проведения совещаний и переговоров по конфиденциальным вопросам | | |
| 5 | | Организационная защита информации в процессе издательской, рекламной и выставочной деятельности | | |
| 6 | | Организация работы при осуществлении международного сотрудничества | | |
| 7 | | Организация режима защиты конфиденциальной информации при опубликовании материалов в открытой печати | | |
| 8 | | Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации | | |
| 9 | | Порядок работы с конфиденциальными документами | | |
| **Семинарские занятия** | | | | | **6** | 2 |
| **Практическая работа** | | | | | **6** | 3 |
| 1 | | Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих ГТ | | |  |
| 2 | | Составление инструктажа персонала | | |
| 3 | | Создание журнала учета сотрудников по допуску к конфиденциальной информации | | |
| 4 | | Составление списка документов для регистрации конфиденциальной информации | | |
| 5 | | Составление конфиденциальных документов с учетом грифов секретности | | |
| Тема 1.4. Организация допуска и доступа персонала к конфиденциальной информации | **Содержание** | | | | | **6** | 3 |
| 1 | | Общие положения. Разрешительная система доступа персонала к конфиденциальной информации. | | |  |
| 2 | | Основные положения допуска должностных лиц и граждан к государственной тайне | | |
| 3 | | Порядок оформления и переоформления допуска к государственной тайне. Формы допуска | | |
| 4 | | Основания для отказа лицу в допуске к государственной тайне и условия прекращения допуска | | |
| 5 | | Организация доступа персонала предприятия к сведениям, составляющим государственную тайну, и их носителям | | |
| 6 | | Порядок доступа к конфиденциальной информации командированных лиц | | |
| **Семинарские занятия** | | | | | **2** |  |
| **Практическая работа** | | | | | **4** |  |
| 1 | | Составление и оформление документов на допуск к конфиденциальной информации | | |
| 2 | | Составление инструкции о контроле персонала, имеющего допуск к конфиденциальной информации | | |
| Тема 1.5. Каналы утечки конфиденциальной информации | **Содержание** | | | | | **6** | 2 |
| 1 | | Основы теории информации. Коммуникационный процесс | | |  |
| 2 | | Источники конфиденциальной информации и каналы ее утечки | | |
| 3 | | Порядок вскрытия режимных помещений в случае возникновения чрезвычайных ситуаций | | |
| 4 | | Уничтожение носителей конфиденциальной информации | | |
| 5 | | Учет носителей информации и проектов конфиденциальных документов | | |  |  |
| **Семинарские занятия** | | | | | **2** | 3 |
| **Практическая работа** | | | | | **4** | 3 |
| 1 | | Разработка помещений для работы с конфиденциальной информацией на примере организации | | |
| 2 | | Разработка должностных инструкций и правил допуска в режимные помещения | | |
| Тема 1.6. Организация контроля за состоянием защиты конфиденциальной информации на предприятии | **Содержание** | | | | | **6** | 2 |
| 1 | | Понятие и основные объекты контроля | | |  |
| 2 | | Основные задачи и методы контроля | | |
| 3 | | Отдельные аспекты контроля за состоянием защиты информации | | |
| 4 | | Использование результатов контроля | | |
| 5 | | Контроль за выполнением требований внутри объектового режима при работе с конфиденциальными сведениями | | |  |  |
|  | |  | | |  |  |
| **Семинарские занятия** | | | | | **4** | 3 |
| **Практическая работа** | | | | | **2** | 3 |
| 1 | | Составление актов проверки наличия конфиденциальных документов на предприятии | | |
| 2 | | Составление документов о проведении проверки на предприятии | | |
| Тема 1.7. Обеспечение сохранности конфиденциальной информации | **Содержание** | | | | | **8** | 2 |
| 1 | | Общие положения. Порядок работы с конфиденциальной информацией, представленной в электронном виде. | | |  |
| 2 | | Определение конфиденциальной информации и обозначение бумажных документов, содержащих конфиденциальную информацию, и сроков ее защиты. | | |
| 3 | | Организация работы с бумажными документами, имеющих гриф "Конфиденциально" | | |
| 4 | | Порядок обеспечения сохранности документов и дел (архивов), содержащих конфиденциальную информацию. | | |
| 5 | | Обязанности сотрудников Организации, работающих с конфиденциальными сведениями и их ответственность за ее разглашение. | | |
| **Семинарские занятия** | | | | | **4** |  |
| **Практическая работа** | | | | | **4** | 3 |
|  | | Составление списка документов для передачи в архив | | |  |  |
|  | | Подготовка документов для передачи в архив | | |  |  |
|  | | Составление актов о приеме (передаче) документов в архив | | |  |  |
| **Самостоятельная работа при изучении МДК 01.03.**   * Подготовка доклада. * Составление опорного конспекта. * Составление тезисов. * Работа с электронными информационными ресурсами и ресурсами Internet * Решение вариативных задач и упражнений. * Работа с компьютерными программами. | | | | | | **26** |  |
| **Примерная тематика внеаудиторной самостоятельной работы**   * Подготовка презентации по теме «Концепция построения системы защищенного документооборота предприятия». * Составление терминологического словаря по дисциплине «Защита и обработка конфиденциальных документов». * Подготовка рефератов. * Чтение дополнительной литературы. * Ответы на контрольные вопросы. * Составление тестовых заданий по темам семинарских занятий. | | | | | |  |  |
| **Виды работ по учебной практике**   * Составление перечня информации, циркулирующей на предприятии * Освоение особенностей учета, обработки, хранения, передачи, использования различных носителей конфиденциальной информации * Определение порядка организации и проведения рабочих совещаний * Определение требований режима защиты информации при приеме в организации посетителей * Определение методов защиты информации в рекламной и выставочной деятельности * Определение требований режима защиты конфиденциальной информации при опубликовании материалов в открытой печати * Определение организации работ по защите информации при осуществлении международного сотрудничества | | | | | | **18** |  |
| **Раздел 4 ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта** | |  | | | | **150** |  |
| **МДК.01.04.** **Разработка, внедрение и сопровождение политики безопасности** | |  | | | | **150** |  |
| Тема 1.1. Политика информационной безопасности как элемент административного уровня информационной безопасности | | **Содержание** | | | | **2** | 2 |
| 1 | | Введение. Политика информационной безопасности как элемент административного уровня информационной безопасности. Уровни детализации политики информационной безопасности | |  |
| **Семинарские занятия** | | | | **2** |  |
| Тема 1.2. Международные и отечественные стандарты в области информационной безопасности, затрагивающие вопросы политики ИБ | | **Содержание** | | | | **2** | 3 |
| 1 | | Обзор стандартов в области информационной безопасности: ISO 17799:2005, ISO/IEC 13335-1:2004, BS 7799-3:2006, ГОСТ Р ИСО/МЭК 27001 | |  |
| **Семинарские занятия** | | | | **2** | 3 |
| Тема 1.3. Назначение и цели политики информационной безопасности | | **Содержание** | | | | **2** | 3 |
| 1 | | Назначение и цели документа. Законодательная основа документа Политики информационной безопасности. Требования к политике безопасности | |  |
| **Семинарские занятия** | | | | **2** |
| Тема 1.4. Объекты защиты | | **Содержание** | | | | **8** | 3 |
| 1 | | Структура, состав и размещение основных объектов защиты, информационные  связи | |  |  |
| 2 | | Пути реализации непреднамеренных/преднамеренных искусственных (субъективных) угроз безопасности информации. | |
| **Семинарские занятия** | | | | **2** |
| **Практическая работа** | | | | **4** | 3 |
| 1 | | Выявление угроз информационной безопасности и их источников | |
| 2 | | Создание модели нарушителя информационной безопасности организации | |
| Тема 1.5. Правила политики безопасности | | **Содержание** | | | | **6** | 3 |
| 1 | | Регламентация доступа в помещения. Разработка правил политики безопасности кадровой системы. Регламентация допуска сотрудников к использованию информационных ресурсов | |  |  |
| **Семинарские занятия** | | | | **2** |
| **Практическая работа** | | | | **4** |
| 1 | | Контроль доступа в помещения организации | |  |
| 2 | | Разработка правил для политики безопасности управления доступом для определенной организации  Разработка правил политики безопасности кадровой системы | |  |
| Тема 1.6. Правила политики безопасности для аппаратных средств | | **Содержание** | | | | **3** | 3 |
| 1 | | Правила политики безопасности для аппаратных средств | |  | 3 |
| **Семинарские занятия** | | | | **1** |
| **Практическая работа** | | | | **2** |
| 1 | | Разработка правил политики безопасности для аппаратных средств | |  |
| Тема 1.7. Правила политики безопасности для программных средств | | **Содержание** | | | | **3** | 3 |
| 1 | | Назначение правил политики безопасности для программных средств | |  | 3 |
| **Семинарские занятия** | | | | **1** |
| **Практическая работа** | | | | **2** |
| 1 | | Разработка правил политики безопасности для программных средств | |  |
| Тема 1.8. Правила политики безопасности внешнего доступа | | **Содержание** | | | | **6** | 3 |
| 1 | | Разработка правил политики безопасности внешнего доступа. Удаленный доступ. Доступ к сети Интернет | |  | 3 |
| **Семинарские занятия** | | | | **2** |
| **Практическая работа** | | | | **4** |
| 1 | | Разработка правил политики безопасности использования удаленного доступа к системам организации | |  |
| 2 | | Разработка правил политики безопасности доступа к сети Интернет. Рекомендуемые правила пользования электронной почтой | |  |
| Тема 1.9. Работа с криптографическими системами | | **Содержание** | | | | **4** | 3 |
| 1 | | Работа с криптографическими системами | |  | 3 |
| **Семинарские занятия** | | | | **2** |
| **Практическая работа** | | | | **2** |
| 1 | | Разработка правил работы с криптографическими системами | |  |
| Тема 1.10. Правила политики безопасности внекомпьютерных информационных ресурсов | | **Содержание** | | | | **6** | 3 |
| 1 | | Разработка правил политики безопасности внекомпьютерных информационных ресурсов | |  | 3 |
| **Семинарские занятия** | | | | **2** |
| **Практическая работа** | | | | **4** |
| 1 | | Разработка правил политики безопасности внекомпьютерных информационных ресурсов | |  |
| 2 | | Разработка правил политики безопасности для реализации физической безопасности | |  |
| Тема 1.11.Организационная основа реализации документа политики ИБ | | **Содержание** | | | | **4** | 3 |
| 1 | | Организационная основа деятельности по обеспечению информационной безопасности.  Ответственность за соблюдение положений Политики.  Контроль за соблюдением положений Политики.  Дисциплинарные меры. | |  | 3 |
| **Семинарские занятия** | | | | **2** |
| **Практическая работа** | | | | **2** |
| 1 | | Реализация контроля за соблюдением положений Политики  Разработка дисциплинарных мер в организации | |  |
| **Самостоятельная работа при изучении при изучении МДК 01.04.**   1. Подготовка доклада. 2. Составление опорного конспекта. 3. Составление тезисов. 4. Работа с электронными информационными ресурсами и ресурсами Internet 5. Решение вариативных задач и упражнений. | | | | | | **32** |  |
| **Примерная тематика внеаудиторной самостоятельной работы**   1. Создание презентации «Административный уровень информационной безопасности» 2. Выполнение упражнений: «Разграничение уровней политики информационной безопасности» 3. Написание эссе по теме Решения разных уровней политики информационной безопасности» 4. Выполнение упражнений «Обработка информации текстов международных и отечественных стандартов» 5. Создание сравнительной таблицы «Политика информационной безопасности в международных и отечественных стандартах» 6. Написание реферата «Использование документа политики ИБ в качестве основы для построения комплексной системы информационной безопасности». 7. Выполнение упражнений по теме «Принципы создания комплексных систем обеспечения безопасности информации». 8. Выполнение расчетно-графической работы «Составление частной модели угроз для организации» 9. Выполнение упражнений по теме «Категории информационных ресурсов, подлежащих защите» 10. Создание опорного конспекта по теме «Утечка информации по техническим каналам» 11. Создание таблицы для систематизации «Меры обеспечения информационной безопасности» 12. Выполнение упражнений по теме «Методы и средства защиты информационного ресурса» 13. Выполнение упражнений по теме «Выявление ответственных лиц за реализацию политик ИБ разных уровней». 14. Создание презентации «Основные принципы построения системы информационной безопасности организаций разных типов» 15. Выполнение упражнений по теме «Выявление требований к аппаратным и программным средствам организации» 16. Создание презентации по теме «Антивирусные средства». 17. Выполнение упражнений по теме «Подбор антивирусного средства для конкретных организаций». 18. Выполнение упражнений по теме «Использование электронной почты в организации». 19. Создание Web-страницы «Правила подсоединения к Internet» 20. Электронное конспектирование «Обзор криптографических средств» 21. Выполнение упражнений по теме «Подбор средств защиты речевой информации» 22. Создание кроссворда «Термины и определения документа Политики ИБ» 23. Выполнение упражнений по теме «Решение правовых и организационных ситуаций, связанных с реализацией Политики ИБ» 24. Подготовка к деловой игре «Реализация политики информационной безопасности в банке» 25. Подготовка и проведение проекта документа Политики информационной безопасности. | | | | | |  |  |
| **Виды работ по учебной практике**   * Анализ структуры организации и ее информационных потоков * Выявление угроз информационной безопасности организации * Разработка модели нарушителя информационной безопасности * Выделение уровней детализации политики информационной безопасности | | | | | | **18** |  |
| **Виды работ по практике** **по профилю специальности**   * Анализ структуры организации и информационных процессов. * Выявление опасностей и угроз организации. * Анализ структуры и типов защищаемой информации, по видам тайны и степеням конфиденциальности. * Анализ кадрового и ресурсного обеспечения защиты информации на предприятии. * Анализ существующей системы защиты объекта. * Оценка степени защищенности объекта; * Использование законодательных и нормативных документов при разработке политики информационной безопасности; * Разработка нормативных документов необходимых для организации работы с персоналом, имеющим доступ к конфиденциальной информации. * Разработка политики информационной безопасности | | | | | | **144** |  |

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).

# **УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

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

Реализация профессионального модуля предполагает наличие учебного кабинетов «Информационной безопасности», «Вычислительной техники», «Документоведения и документационного обеспечения управления».

Оборудование учебных кабинетов:

посадочные места по количеству обучающихся, рабочее место преподавателя; рабочие программы по МДК, методическая литература; комплект учебной литературы по дисциплине; электронные учебные издания; демонстрационные печатные пособия; экранно-звуковые пособия; электронное сопровождение учебных занятий; дидактический материал по темам; контрольно-измерительные материалы; компьютерные тестовые программы; компьютеры с лицензионным программным обеспечением, принтер, сканеры, телевизор, локальная сеть, комплект учебно-методической документации.

**4.2. Информационное обеспечение обучения**

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

**Основные источники:**

Партыка Т.Л. Информационная безопасность : учебн. пособие для спо / Т.Л. Партыка, И.И. Попов. - М.: ФОРУМ: ИНФРА-М, 2011.

**Дополнительные источники:**

1. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян . – М.: ФОРУМ, 2011. – 256 с.
2. Пшенко А.В. Документационное обеспечение управления. ОИЦ "Академия" 2010
3. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин – М.: ФОРУМ ИНФРА-М, 2014. – 416 с.

**Интернет ресурсы:**

* [www.avosp.ru](http://www.avosp.ru/)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)

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

Программа профессионального модуля ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта реализуется в течение 2-х семестров последнего курса обучения.

Освоению данного модуля предшествует изучение дисциплин общего гуманитарного и социально-экономического, математического и естественнонаучного, общепрофессионального циклов, таких как*:* «Информационные технологии», «Документоведение», «Документационное обеспечение управления», «Архивоведение», «Основы информационной безопасности», «Организационные основы деятельности организации», и профессиональных модулей: ПМ.02 «Организация и технология работы с конфиденциальными документами», ПМ.03 «Программно-аппаратные и технические средства защиты информации».

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.

При работе над курсовым проектом студентам оказываются консультации.

**4.4. Кадровое обеспечение образовательного процесса**

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарному курсу**:** наличие высшего профессионального образования, соответствующего профилю модуля и специальности 10.02.01 Организация и технология защиты информации.

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.

# **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 1.1 Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации. | - соответствие собранного материала, необходимого для выработки решений по обеспечению защиты информации реальному положению дел;  - соблюдение методики анализа материала для выработки оптимальных решений по обеспечению защиты информации;  - точность выявления возможных каналов утечки конфиденциальной информации; | **Входной контроль**:  - тестирование  **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 и лабораторных работ;  **Итоговый контроль**:  Комплексный экзамен по МДК.01.02 и МДК.01.03  Комплексный экзамен по МДК.01.01 и МДК.01.04  Комплексный зачет по учебной практике и практике по профилю специальности.  Квалификационный экзамен по профессиональному модулю.  Проверка сформированности компетенций и готовности к выполнению вида профессиональной деятельности  Участие в планировании и организации работ по обеспечению защиты объекта |
| ПК 1.2 Участвовать в разработке программ и методик организации защиты информации на объекте. | - точность выявления зон доступа по типу и степени конфиденциальности работ;  - точность использования критериев подбора и расстановки сотрудников подразделений защиты информации |
| ПК 1.3 Осуществлять планирование и организацию выполнения мероприятий по защите информации. | -соблюдение требований к процессу проведения инструктажа персонала по организации работы с конфиденциальной информацией;  - соблюдение требований при выполнении мероприятий по защите информации; |
| ПК 1.4 Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности. | -точное соответствие алгоритму процесса внедрения решений на объекте; |
| ПК 1.5 Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации. | -соответствие методов обработки, хранения, использования и передачи носителей степени конфиденциальности информации;  -соблюдение требований к учету носителей конфиденциальной информации; |
| ПК 1.6 Обеспечивать технику безопасности при проведении организационно-технических мероприятий. | -соответствие проводимых организационно-технических мероприятий требованиям техники безопасности; |
| ПК 1.7 Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите. | - составление и соблюдение графика проведения проверок;  - точность выявления документов, подлежащих проверке; |
| ПК 1.8 Проводить контроль соблюдения персоналом требований режима защиты информации. | - правильность применения различных способов контроля персонала с целью соблюдения требований режима защиты информации; |
| ПК 1.9 Участвовать в оценке качества защиты объекта. | -правильность выделения зон доступа по типу и степени конфиденциальности работ;  -правильность определения угроз;  -грамотное объяснение соответствия (или несоответствия) примененных методов защиты объекта реальным угрозам; |

**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, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности. | -грамотное использование научной литературы для выполнения профессиональных обязанностей;  - рейтинг участия в профессиональных олимпиадах, конкурсах, семинарах;  - правильность изложения сущности будущей профессии | 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, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. | - соответствие выбранных методов целям задания;  - рациональность планирования и организации деятельности по решению профессиональных задач | 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 Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. | - правильность определения угроз;  - соответствие выбора способа защиты с реальными угрозами;  - правильность проведения анализа ситуации по заданным критериям и определение рисков;   * правильность оценивания последствий принятых решений; |
| ОК 4 Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. | - результативность поисковых запросов;  - результативность анализа и синтеза информации;  - корректное использование информационных источников для анализа, оценки и извлечения информационных данных, необходимых для решения профессиональных задач; |
| ОК 5 Использовать информационно-коммуникационные технологии в профессиональной деятельности. | - рациональность выбора и использования ИКТ в соответствии с поставленными целями | 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, эффективно общаться с коллегами, руководством, потребителями. | -результативность участия в коллективных творческих проектах;  - результативность зашиты творческого проекта | 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 Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. | - ответственное отношение к результатам выполнения профессиональных обязанностей членами команды;  - проведение самоанализа и коррекции результатов команды; |
| ОК 8 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. | - рейтинг участия в профессиональных олимпиадах, конкурсах, семинарах, научно-исследовательской деятельности;  - грамотное использование научной литературы при выполнение рефератов, заданий для самостоятельной работы, курсовой работы (проекта);  - рациональное планирование, организация собственной деятельности;   * результативность коррекции результатов в области образовательной деятельности; | 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 Ориентироваться в условиях частой смены технологий в профессиональной деятельности. | - рейтинг участия в профессиональных олимпиадах, конкурсах, семинарах, научно-исследовательской деятельности;  - рейтинг участия в интернет-сообществах, группах, ведения страницы, блога и т.д., посвященных технологиям, в области информационной безопасности. |
| ОК 10 Применять математический аппарат для решения профессиональных задач. | - точность построения математической модели объекта, процесса, системы для эффективного решения профессиональных задач; | Интерпретация результатов наблюдений за деятельностью студента в процессе освоения программы профессионального модуля;  - выполнение заданий для самостоятельной работы;  -выполнение практических работ;  - выполнение творческой работы. |
| ОК 11 Оценивать значимость документов, применяемых в профессиональной деятельности. | - грамотно оперирует понятиями, применяемыми в документах из области профессиональной деятельности;  - правильность определения приоритетов документов, применяемых в профессиональной деятельности; |
| ОК12 Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность. | - правильность изложения структуры федеральных органов исполнительной власти, обеспечивающих информационную безопасность; | Интерпретация результатов наблюдений за деятельностью студента в процессе освоения программы профессионального модуля;  - выполнение заданий для самостоятельной работы;  -выполнение практических работ;  -выполнение рефератов, докладов и презентаций;  - выполнение творческой работы. |