Областное государственное бюджетное профессиональное образовательное учреждение

«Смоленская академия профессионального образования»

Утверждаю

Зам. директора по УМР

\_\_\_\_\_\_\_\_\_\_\_\_\_Н. В. Судденкова

**Комплект контрольно-оценочных средств**

**по профессиональному модулю**

ПМ.03 **Программно-аппаратные и технические средства защиты информации**

для специальности 090905 Организация и технология защиты информации по программе базовой подготовки

Смоленск 2014

Комплект контрольно-оценочных средств по профессиональному модулю ПМ.03 Программно-аппаратные и технические средства защиты информации для специальности 090905 Организация и технология защиты информации по программе базовой разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 090905 Организация и технология защиты информации по программе базовой подготовки.

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

Разработчики:

*Ромашкова И.А.,* преподаватель ОГБПОУ СмолАПО

Согласовано с работодателем \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рассмотрено на заседании кафедры Информационных технологий

Протокол № \_\_\_\_\_\_ от «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2014 г.

Зав. кафедрой (декан) \_\_\_\_\_\_\_\_\_\_\_\_ */*В.Г. Малахова*/*

Рассмотрено научно-методическим советом ОГБПОУ «Смоленская академия профессионального образования»

Протокол № \_\_\_\_\_\_ от «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2014 г.

\_\_\_\_\_\_\_\_\_\_\_\_\_

**Содержание**

[1. Паспорт комплекта контрольно-оценочных средств по профессиональному модулю 4](#_Toc406919758)

[1.1. Результаты освоения программы профессионального модуля 4](#_Toc406919759)

[1.1.1 Вид профессиональной деятельности 4](#_Toc406919760)

[1.1.2 Профессиональные и общие компетенции 4](#_Toc406919761)

[1.1.3 Практический опыт, умения, знания 6](#_Toc406919762)

[1.2 Формы промежуточной аттестации при освоении программы профессионального модуля 7](#_Toc406919763)

[2. Паспорт контрольно-измерительных материалов для проведения промежуточной аттестации по междисциплинарным курсам 9](#_Toc406919764)

[2.1 Область применения 9](#_Toc406919765)

[2.2. Комплект контрольно-измерительных материалов для проведения промежуточной аттестации по междисциплинарным курсам 9](#_Toc406919766)

[2.2.1 Условия выполнения задания 9](#_Toc406919767)

[Максимальное время выполнения задания – 1академический час. 9](#_Toc406919768)

[2.2.2 Образцы заданий 9](#_Toc406919769)

[2.2.3 Критерии оценки 10](#_Toc406919770)

[3. Паспорт материалов для оценки результатов практики 12](#_Toc406919771)

[3.1 Область применения 12](#_Toc406919772)

[3.2 Виды работ для оценки результатов практики 13](#_Toc406919773)

[3.3 Критерии оценки 14](#_Toc406919774)

[4. Паспорт контрольно-оценочных материалов экзамена (квалификационного) 16](#_Toc406919775)

[4.1 Область применения 16](#_Toc406919776)

[4.2 Аттестационные испытания 17](#_Toc406919777)

[4.2.1 Проверяемые результаты 17](#_Toc406919778)

[4.2.2 Основные требования 18](#_Toc406919779)

[4.2.3 Критерии оценки 19](#_Toc406919781)

[5. Информационное обеспечение 21](#_Toc406919782)

# **1. Паспорт комплекта контрольно-оценочных средств по профессиональному модулю**

## 1.1. Результаты освоения программы профессионального модуля

### *1.1.1 Вид профессиональной деятельности*

Результатом освоения программы профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности «Применение программно-аппаратных и технических средств защиты информации».

### *1.1.2 Профессиональные и общие компетенции*

В результате освоения программы профессионального модуля, у обучающегося должны быть сформированы следующие профессиональные компетенции (ПК) и общие компетенции (ОК).

Таблица 1. Показатели оценки сформированности ПК

|  |  |
| --- | --- |
| **Профессиональные компетенции**  (должны быть сформированы в полном объеме) | **Показатели оценки результата** |
| ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах. | Соблюдение методики применения программно-аппаратных и технических средств защиты информации; |
| ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов. | * Соответствие установленных систем и средств защиты информации защищаемых объектов правилам эксплуатации; * Соответствие режима эксплуатации систем и средств защиты информации защищаемых объектов правилам эксплуатации. |
| ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты. | * Точное соответствие выполняемых работ на защищаемых объектах регламенту; * Точное определение факта и причин отказа оборудования средств защиты информации. |
| ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов. | * Соответствие построенной модели угроз наиболее вероятным реальным угрозам; * Аргументированность выявления угроз безопасности, соответствие выявленных угроз величинам ущерба от них. |

Таблица 2. Показатели оценки сформированности ОК

|  |  |
| --- | --- |
| **Общие компетенции**  (возможна частичная сформированность) | **Показатели оценки результата** |
| ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности | Точно излагает сущность, особенности и задачи будущей деятельности, активно выполняет профессиональную деятельность в области обеспечения информационной безопасности |
| ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество | Рационально планирует и реализует профессиональную работу и выбирает методы для решения профессиональных задач |
| ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность | Точно выстраивает алгоритм действий и предусматривает риски в нестандартных ситуациях |
| ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития | Результативность поиска и оценки информации для постановки и решения профессиональных задач, профессионального и личностного развития |
| ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности | Владеет соответствующими информационно-коммуникационные технологиями в профессиональной деятельности |
| ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями | Адекватность и результативность поведения в коллективе, владение приемами коммуникации |
| ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий | Проявление ответственности за результат |
| ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации | Обоснованность поставленных задач, развитие навыков самоанализа, планирование повышения квалификации |
| ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности | Рациональность поиска в условиях изменения технологий в профессиональной деятельности. |
| ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей) | Выполнение требований по исполнению воинской обязанности |
| ОК 11. Применять математический аппарат для решения профессиональных задач | Рациональность применения математического аппарата для решения профессиональных задач |
| ОК 12. Оценивать значимость документов, применяемых в профессиональной деятельности | Ориентируется и учитывает изменения нормативных документов |
| ОК 13. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность | Ориентируется в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность |

### *1.1.3 Практический опыт, умения, знания*

В результате освоения программы профессионального модуля обучающийся должен освоить следующие дидактические единицы:

* иметь практический опыт;
* уметь;
* знать.

Таблица 3. Показатели оценки сформированности практического опыта

|  |  |
| --- | --- |
| **Практический опыт** | **Показатели оценки результата** |
| ПО 1. Участия в эксплуатации систем и средств защиты информации защищаемых объектов | Соблюдение требований по эксплуатации систем и средств защиты информации |
| ПО 2. Применения технических средств защиты информации | Соблюдение требований и регламентов при применении технических средств защиты информации |
| ПО 3. Выявления возможных угроз информационной безопасности объектов защиты | Соответствие выявленных угроз информационной безопасности объекта реально существующим угрозам |

Таблица 4. Показатели оценки освоения умений

|  |  |
| --- | --- |
| **Умения** | **Показатели оценки результата** |
| У1. Работать с техническими средствами защиты информации | Техничность работы технических средств защиты информации |
| У2. Работать с защищенными автоматизированными системами | Техничность применения программно-аппаратных защиты информации |
| У3. Передавать информацию по защищенным каналам связи | Соблюдение регламента передачи информации по защищенным каналам связи |
| У4. Фиксировать отказы в работе средств вычислительной техники | Результативность в определении отказов в работе средств вычислительной техники |

Таблица 5. Показатели оценки усвоения знаний

|  |  |
| --- | --- |
| **Знания** | **Показатели оценки результата** |
| Зн1. Виды, источники и носители защищаемой информации | Полнота изложения видов, источников и носителей защищаемой информации |
| Зн2. Источники опасных сигналов | Полнота изложения источников опасных сигналов |
| Зн3. Структуру, классификацию и основные характеристики технических каналов утечки информации | Правильно воспроизводит классификацию, структуру и основные характеристики технических каналов утечки информации |
| Зн4. Классификацию технических разведок и методы противодействия им | Полнота изложения классификации технических разведок и методов противодействия им |
| Зн5. Методы и средства технической защиты информации | Правильность изложения методов и средств технической защиты информации |
| Зн6. Методы скрытия информации | Правильность изложения методов скрытия информации |
| Зн7. Программно-аппаратные средства защиты информации | Полнота изложения программно-аппаратных средств защиты информации |
| Зн8. Структуру подсистемы безопасности операционных систем и выполняемые ею функции | Правильность изложения структуры подсистемы безопасности операционных систем и выполняемых ею функции |
| Зн9. Средства защиты в вычислительных сетях | Полнота изложения средств защиты в вычислительных сетях |
| Зн10. Средства обеспечения защиты информации в системах управления базами данных | Полнота изложения средств обеспечения защиты информации в системах управления базами данных |
| Зн11. Критерии защищенности компьютерных систем | Правильность изложения критериев защищенности компьютерных систем |
| Зн12. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов | Правильность изложения методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов |

## 1.2 Формы промежуточной аттестации при освоении программы профессионального модуля

Формой промежуточной аттестации по итогам освоения программы профессионального модуля является экзамен (квалификационный).

Итогом экзамена (квалификационного) является однозначное решение: вид профессиональной деятельности освоен / не освоен.

Для элементов, входящих в состав профессионального модуля (междисциплинарные курсы, учебная практика и практика по профилю специальности), предусмотрена промежуточная аттестация в форме комплексных дифференцированных зачетов.

Таблица 6. Формы промежуточной аттестации

|  |  |
| --- | --- |
| **Элементы модуля, профессиональный модуль** | **Формы промежуточной аттестации** |
| МДК 03.01 Технические методы и средства, технологии защиты информации | Комплексный  дифференцированный  зачет |
| МДК 03.02 Программно-аппаратные средства защиты информации |
| Учебная практика | Комплексный  дифференцированный  зачет |
| Производственная практика |
| **ПМ. 03** | **Квалификационный экзамен** |

Комплект контрольно-оценочных средств по профессиональному модулю ПМ.03 Программно-аппаратные и технические средства защиты информации:

* контрольно-измерительные материалы для проведения промежуточной аттестации по междисциплинарным курсам;
* контрольно-оценочные материалы для проведения экзамена (квалификационного).

Средствами оценки результатов практики по профилю специальности является формализованное наблюдение и анализ представленных материалов в соответствии с п. 7.7 Положения о практике студентов, осваивающих основные профессиональные образовательные программы среднего профессионального образования в ОГБПОУ «Смоленская академия профессионального образования».

# **2. Паспорт контрольно-измерительных материалов для проведения промежуточной аттестации по междисциплинарным курсам**

## 2.1 Область применения

Контрольно-измерительные материалы для проведения промежуточной аттестации по МДК 03.01 Технические методы и средства, технологии защиты информации, МДК 03.02 Программно-аппаратные средства защиты информации предназначены для проверки результатов освоения умений и усвоения знаний в соответствии с программой профессионального модуля Программно-аппаратные и технические средства защиты информации.

## 2.2. Комплект контрольно-измерительных материалов для проведения промежуточной аттестации по междисциплинарным курсам

### *2.2.1 Условия выполнения задания*

Место проведения промежуточной аттестации – учебная аудитория.

Используемое оборудование – персональный компьютер, устройства программно-аппаратной защиты информации, техническая документация.

Максимальное время выполнения задания – 1академический час.

Раздаточные материалы – структуры организаций

### *2.2.2 Образцы заданий*

Таблица 7. Типовые задания для проведения промежуточной аттестации по МДК

|  |  |  |
| --- | --- | --- |
| **Типовое задание** | **Коды проверяемых результатов** | |
| **У** | **Зн** |
| Выявление и анализ возможных угроз информационной безопасности объекта, определение технических каналы утечки информации объекта, оценка вероятности их существования и выбор способов закрытия выявленных каналов утечки информации. | У1, У3 | Зн 3, Зн 5,  Зн 9, Зн 12 |
| Выявление и анализ возможных угроз информационной безопасности объекта, определение технических каналов утечки информации объекта и составление плана регламентных работ по обслуживанию средств защиты. | У1, У3 | Зн 3, Зн 5,  Зн 7, Зн 8, Зн 12 |
| Выявление и анализ возможных угроз информационной безопасности АС, определение адекватной политики безопасности компьютера, выбор программно-аппаратных средств защиты информации и настройка их | У2 | Зн 3, Зн 5,  Зн 7, Зн 8, Зн 9,  Зн 11, Зн 12 |

Умение 4, а также знания 1, 2, 4, 6, 10 проверяются по результатам выполнения практических работ при реализации программ междисциплинарных курсов.

### *2.2.3 Критерии оценки*

Оценка «5» ставится в случае, если перечислены все виды угроз объекта защиты, определены технические каналы утечки информации, оценена вероятность их существования, обоснован выбор технических и программно-аппаратных средств защиты объекта, осуществлена их установка и составлен план регламентных работ по обслуживанию средств защиты.

Оценка «4» ставится в случае, если перечислены все виды угроз объекта защиты, определены технические каналы утечки информации, обоснованы, но допущены не значительные неточности в оценке степени их вероятности; не полностью обоснован выбор технических и программно-аппаратных средств защиты объекта, осуществлена их установка и составлен план регламентных работ по обслуживанию средств защиты.

Оценка «3» ставится в случае, если перечислены не все виды угроз объекта защиты, определены не все технические каналы утечки информации; допущены не значительные неточности в оценке степени их вероятности; не полностью обоснован выбор технических и программно-аппаратных средств защиты объекта; при установке допущены значительные неточности; составлен план регламентных работ по обслуживанию средств защиты.

Оценка «2» ставится в случае, если не перечислены виды угроз объекта защиты, не определены технические каналы утечки информации; допущены значительные неточности в оценке степени их вероятности; не обоснован выбор технических и программно-аппаратных средств защиты объекта; установка программно-аппаратных средств защиты информации не выполнена.

# **3. Паспорт материалов для оценки результатов практики**

## 3.1 Область применения

Материалы достижений обучающихся в период прохождения учебной практики и практики по профилю специальности предназначены для проверки результатов сформированности:

* практического опыта;
* профессиональных компетенций ПК 3.1 Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах, ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов, ПК 3.3 Проводить регламентные работы и фиксировать отказы средств защиты, ПК 3.4 Выявлять и анализировать возможные угрозы информационной безопасности объектов;
* общих компетенций 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 Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей), ОК 11 Применять математический аппарат для решения профессиональных задач, ОК 12 Оценивать значимость документов, применяемых в профессиональной деятельности, ОК 13 Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

## 3.2 Виды работ для оценки результатов практики

Таблица 8. Виды работ, выполняемых в период прохождения учебной практики

|  |  |  |  |
| --- | --- | --- | --- |
| Виды работ и требования к их выполнению | Коды проверяемых результатов | | |
| ПК | ОК | ПО |
| Выявление технических каналов утечки информации и выбор способов их защиты на примерах организаций | – | – | ПО 1  ПО 2 |
| Выявления возможных угроз информационной безопасности объектов защиты | – | – | ПО 3 |
| Установка и настройка программно-аппаратных средств защиты информации | – | – | ПО 1  ПО 2 |

Таблица 8. Виды работ, выполняемых в период прохождения практики по профилю специальности

|  |  |  |  |
| --- | --- | --- | --- |
| **Виды работ и требования к их выполнению** | **Коды проверяемых результатов** | | |
| **ПК** | **ОК** | **ПО** |
| Анализ объекта защиты  *Требования к выполнению:* использование соответствующих структурных схем организаций | ПК 3.4  ПК 3.2 | ОК 1, ОК 2,  ОК 3, ОК 6, ОК 9, ОК 11,  ОК 12 | ПО 1,  ПО 3 |
| Выявление возможных угроз информационной безопасности объекта защиты  *Требования к выполнению:* соблюдение требований классификаций угроз и оценки их актуальности | ПК 3.4 | ОК 1, ОК 2,  ОК 3, ОК 6, ОК 9, ОК 11,  ОК 12 | ПО 3 |
| Анализ инженерно-технической защиты объекта  *Требования к выполнению:* использование соответствующих методик | ПК 3.2  ПК 3.3 | ОК 1, ОК 2,  ОК 3, ОК 6, ОК 9, ОК 11,  ОК 12 | ПО 1,  ПО 3 |
| Анализ программно-аппаратной защиты объекта  *Требования к выполнению:* использование соответствующих методик | ПК 3.2  ПК 3.3 | ОК 1, ОК 2,  ОК 3, ОК 6, ОК 9, ОК 11,  ОК 12 | ПО 1,  ПО 3 |
| Разработка мероприятий по совершенствованию технической и программно-аппаратной защите информации  *Требования к выполнению:* соблюдение нормативных требований | ПК 3.1,  ПК 3.4 | ОК 1, ОК 2,  ОК 3, ОК 6, ОК 9, ОК 11,  ОК 12 | ПО 2 |

## 

## 3.3 Критерии оценки

Оценка «5» ставится в случае, если классифицированы все виды угроз в организации и аргументировано осуществлено профессиональное толкование нормативно-правовых документов для разработки правил безопасности различных систем, разработаны правила политики информационной безопасности для организации, точно оценена степень защищенности организации.

Оценка «4» ставится в случае, если перечислены все виды угроз в организации, разработка правил безопасности различных систем организации соответствует основным нормативно-правовым документам, обоснованы, но допущены незначительные неточности в оценке степени защищенности организации; профессиональное толкование нормативно-правовых актов для разработки правил безопасности различных систем, на основании которых составлены правила политики безопасности различных систем организации.

Оценка «3» ставится в случае, если разработка правил безопасности различных систем организации соответствует основным нормативно-правовым документам, обоснованы, но допущены значительные неточности, выявлены не все виды угроз; профессиональное толкование нормативно-правовых актов для составления правил безопасности, недостаточно четкое и полное представление основных правил политики безопасности, допущены существенные ошибки при оценке степени защищенности организации.

Оценка «2» ставится в случае, если разработка правил безопасности различных систем организации не соответствует основным нормативно-правовым документам, не осуществлено профессиональное толкование нормативно-правовых документов для разработки правил безопасности различных систем, не разработаны правила политики информационной безопасности для организации, не выявлены угрозы, отсутствует оценка степени защищенности организации.

# **4. Паспорт контрольно-оценочных материалов экзамена (квалификационного)**

## 4.1 Область применения

Контрольно-оценочные материалы предназначены для проверки результатов сформированности:

* профессиональных компетенций ПК 3.1 Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах, ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов, ПК 3.3 Проводить регламентные работы и фиксировать отказы средств защиты, ПК 3.4 Выявлять и анализировать возможные угрозы информационной безопасности объектов;
* общих компетенций 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 Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей), ОК 11 Применять математический аппарат для решения профессиональных задач, ОК 12 Оценивать значимость документов, применяемых в профессиональной деятельности, ОК 13 Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

## 4.2 Аттестационные испытания

Экзамен (квалификационный) состоит из аттестационного испытания – защита результатов практики.

**4.2.1 Проверяемые результаты**

* профессиональных компетенций ПК 3.1 Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах, ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов, ПК 3.3 Проводить регламентные работы и фиксировать отказы средств защиты, ПК 3.4 Выявлять и анализировать возможные угрозы информационной безопасности объектов;
* общих компетенций 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 Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей), ОК 11 Применять математический аппарат для решения профессиональных задач, ОК 12 Оценивать значимость документов, применяемых в профессиональной деятельности, ОК 13 Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

**4.2.2 Основные требования**

Требования к структуре и оформлению результатов практики

# Оформление результатов практики выполняется студентом в соответствии с ПОЛОЖЕНИЕМ о практике студентов, осваивающих основные профессиональные образовательные программы среднего профессионального образования в ОГБПОУ «Смоленская академия профессионального образования».

Структурные элементы результатов практики отражают задание, содержание выполненной работы, обобщение результатов работы, оценку полноты решений поставленных задач, краткие выводы по результатам прохождения практики.

Содержание результатов практики следует иллюстрировать схема­ми, таблицами, диаграммами, графиками, фотографиями, рисунками и т.д. Графическому материалу по тексту необходимо давать пояснения.

Требования к защите результатов практики

Защита результатов практики должна продемонстрировать понимание обучающимся сущности и социальной значимости своей будущей профессии, результативность и качество выполненной работы по данному виду профессиональной деятельности (Применение программно-аппаратных и технических средств защиты информации), владение технологиями выполнения различных видов работ, умение обосновывать основные результаты работы.

К защите результатов практики представляется иллюстративный материал в форме презентации, видео и аудио материалов, фотоотчета, проектов нормативных документов и т.п. В процессе защиты раскрывается содержание выполненной работы, анализируются полученные результаты и делаются соответствующие выводы.

Итоговая аттестация слушателя организуется в публичной форме перед комиссией. При невозможности прибытия на защиту на образовательную площадку она может быть организована в формате вебинара. Обсуждение предложенных слушателями мероприятий проходит в рамках круглого стола.

**4.2.3 Критерии оценки**

Оценка «5» ставится в случае, если в содержании работы присутствуют доказательства теоретического и опытного характера, логика изложения материала, анализ по проблематике темы работы; обоснована актуальность тематики работы; грамотно интерпретированы полученные результаты; присутствует собственное мнение в ходе поиска решения проблемы; источники информации являются актуальными; соблюдены каноны научного текста; результаты работы изложены кратко, грамотно и наглядно.

Оценка «4» ставится в случае, если в содержании работы присутствуют доказательства теоретического и опытного характера, логика изложения материала, анализ по проблематике темы работы; обоснована актуальность тематики работы; грамотно интерпретированы полученные результаты; присутствует собственное мнение в ходе поиска решения проблемы; источники информации являются актуальными; соблюдены каноны научного текста; результаты работы изложены кратко, грамотно и наглядно, но допущены некоторые неточности, не влияющие смысл содержания, или незначительные нарушения последовательности изложения.

Оценка «3» ставится в случае, если в содержании работы доказательства теоретического и опытного характера присутствуют частично, логика изложения материала не выдержана, анализ по проблематике темы работы носит частичный характер; актуальность тематики работы обоснована не полно; полученные результаты интерпретированы частично; собственное мнение в ходе поиска решения проблемы отсутствует; источники информации являются актуальными частично; каноны научного текста не соблюдены; при изложении результатов работы допущены нарушения последовательности изложения.

Оценка «2» ставится в случае, если в содержании работы доказательства теоретического и опытного характера присутствуют частично, логика изложения материала не выдержана, анализ по проблематике темы работы не выполнен; актуальность тематики работы обоснована не полно; полученные результаты не интерпретированы; собственное мнение в ходе поиска решения проблемы отсутствует; источники информации являются актуальными частично; каноны научного текста не соблюдены; при изложении результатов работы допущены нарушения последовательности изложения.

Вид профессиональной деятельности считается освоенным, если на экзамене (квалификационном) получена оценка не ниже «удовлетворительно».

**5. Информационное обеспечение**

**Основные источники:**

**Дополнительные источники:**

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Хореев П.Б. Программно-аппаратная защита информации: учебн. пособие для вузов по спец-ти «Информационная безопасность», «Информатика и вычислительная техника» / П.Б. Хореев. – М.: ФОРУМ, 2011. – 351 с.
3. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.
4. Программно-аппаратная защита информации: учеб. Пособие/С.К. Варлатая, М.В. Шаханова. - Владивосток: Изд-во ДВГТУ, 2007.
5. Защита информации в персональном компьютере: учебное пособие/ Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – М.: ФОРУМ, 2012, 368 с.

**Интернет ресурсы:**

* [www.consultant.ru](http://www.consultant.ru)
* www.garant.ru
* [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/)