**ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**Программно-аппаратные и технические средства ЗАЩИТЫ ИНФОРМАЦИИ**

БАЗОВАЯ ПОДГОТОВКА

2014 г.

Программа профессионального модуля ПМ.03 **Программно-аппаратные и технические средства защиты информации**  входит в состав основной профессиональной образовательной программы, разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 090905 Организация и технология защиты информации базовой подготовки.

Организация-разработчик: ОГБПОУ СмолАПО

Разработчик:

Ромашкова И.А., преподаватель ОГБПОУ СмолАПО

Утверждена Научно-методическим советом ОГБПОУ 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** 6](#_Toc316050133)

[**3.** **СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** 7](#_Toc316050134)

[**4.** **УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** 17](#_Toc316050139)

[**5.** **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)** 20](#_Toc316050140)

# **ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

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

**1.1. Область применения программы**

Программа профессионального модуля ПМ.03 Программно-аппаратные и технические средства защиты информации – является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 090905 Организация и технология защиты информации базовой подготовки в части освоения вида профессиональной деятельности (ВПД): **Применение программно-аппаратных и технических средств защиты информации** и соответствующих профессиональных компетенций (ПК):

* применять программно-аппаратные и технические средства защиты информации на защищаемых объектах;
* участвовать в эксплуатации систем и средств защиты информации защищаемых объектов;
* проводить регламентные работы и фиксировать отказы средств защиты;
* выявлять и анализировать возможные угрозы информационной безопасности объектов.

**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:**

* участия в эксплуатации систем и средств защиты информации защищаемых объектов;
* применения технических средств защиты информации;
* выявления возможных угроз информационной безопасности объектов защиты;

**уметь***:*

* работать с техническими средствами защиты информации;
* работать с защищенными автоматизированными системами;
* передавать информацию по защищенным каналам связи;
* фиксировать отказы в работе средств вычислительной техники;

**знать***:*

* виды, источники и носители защищаемой информации;
* источники опасных сигналов;
* структуру, классификацию и основные характеристики технических каналов утечки информации;
* классификацию технических разведок и методы противодействия им;
* методы и средства технической защиты информации;
* методы скрытия информации;
* программно-аппаратные средства защиты информации;
* структуру подсистемы безопасности операционных систем и выполняемые ею функции;
* средства защиты в вычислительных сетях;
* средства обеспечения защиты информации в системах управления базами данных;
* критерии защищенности компьютерных систем;
* методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

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

всего – 620 часа, в том числе:

- максимальной учебной нагрузки обучающегося – 440 часов, включая:

- обязательной аудиторной учебной нагрузки обучающегося – 294 часов;

- самостоятельной работы обучающегося – 146 часа,

- учебной и производственной практики – 180 часов.

# **РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности **Применение программно-аппаратных и технических средств защиты информации**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

|  |  |
| --- | --- |
| **Код** | **Наименование результата обучения** |
| 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. |
| 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.03 Программно-аппаратные и технические средства защиты информации**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 3.1 – ПК 3.4** | **Раздел 1 Технические методы и средства, технологии защиты информации** | **240** | **160** | **80** | - | **80** | - | **18** | **72** |
| **ПК 3.1 – ПК 3.4** | **Раздел 2**  **Программно-аппаратные средства защиты информации** | **200** | **134** | **58** | - | **66** | - | **18** | **72** |
|  | **Производственная практика (по профилю специальности)**, часов |  |  | | | | | |  |
|  | **Всего:** |  | **294** | **138** | - | **146** | - | **36** | **144** |

**3.2. Содержание обучения по профессиональному модулю ПМ.03 Программно-аппаратные и технические средства защиты информации**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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.03 Программно-аппаратные и технические средства защиты информации** |  | | | **572** |  |
| **Раздел 1 ПМ.03 Программно-аппаратные и технические средства защиты информации** |  | | | **240** |  |
| **МДК.03.01.** **Технические методы и средства, технологии защиты информации** |  | | | **240** |
| **Тема1.1 Место технической защиты информации в государственной системе ЗИ в РФ** | **Содержание** | | | **16** | 2 |
| 1 | Цели и задачи ЗИ от УИ по ТК. | |  |
| 2 | Структура, задачи и основные функции государственной системы ЗИ. Ос­нов­ные ру­ко­во­дя­щие, методические и нор­ма­тив­ные до­ку­мен­ты по тех­ни­че­ской ЗИ | |
| **Семинарские занятия** | | | **4** |
| **Практическая работа** | | | **12** | 2 |
| 1 | Изучение законодательной и нормативной базы правового регулирования вопросов защиты информации.  Основные термины и определения в области технической защиты информации | |
| 2 | Изучение положений о государственном лицензировании деятельности в области технической защиты информации | |
| 3 | Изучение положений о сертификации средств защиты информации по требованиям безопасности информации | |
| 4 | Изучение задач и функций органов по технической защите информации в РФ | |
| 5 | Изучение положения о сертификации средств вычислительной техники и связи | |
| **Тема1.2.** **Характеристика информации как объекта защиты** | **Содержание** | | | **16** | 3 |
| 1 | Ви­ды ин­фор­ма­ции, за­щи­щае­мой тех­ни­че­ски­ми сред­ст­ва­ми | |  |
| 2 | Де­ма­ски­рую­щие при­зна­ки объ­ек­тов за­щи­ты | |
| 3 | Ис­точ­ни­ки и но­си­те­ли кон­фи­ден­ци­аль­ной ин­фор­ма­ции | |
| 4 | Ис­точ­ни­ки опас­ных сиг­на­лов. | |
| **Семинарские занятия** | | | **8** |
| **Практическая работа** | | | **8** | 2 |
| 1 | Изучение де­ма­ски­рую­щих при­зна­ков объ­ек­тов за­щи­ты | |
| 2 | Ис­точ­ни­ки и но­си­те­ли кон­фи­ден­ци­аль­ной ин­фор­ма­ции | |
| 3 | Изучение и расчет помех (наводок) в каналах связи при внешней паразитной связи последовательного вида | |
| 4 | Изучение и расчет помех (наводок) в каналах связи при внешней параллельной паразитной связи | |  |  |
| **Тема1.3. Угрозы безопасности информации** | **Содержание** | | | **6** | 2 |
| 1 | Ви­ды уг­роз безо­пас­но­сти ин­фор­ма­ции | |  |
| 2 | Подходы к оценке уровня угрозы | |
| 3 | Факторы, влияющие на возможность реализации угроз. | |
| **Семинарские занятия** | | | **4** |
| **Практическая работа** | | | **2** | 2 |
| 1 | Изучение этапов определения угроз | |
| **Тема 1.4.Тех­ни­че­ские ка­на­лы утеч­ки ин­фор­ма­ции** | **Содержание** | | | **22** | 3 |
| 1 | Структура, классификация и виды ТКУИ | |  |
| 2 | Ха­рак­те­ри­сти­ки ка­на­лов утеч­ки ин­фор­ма­ции | |
| 3 | Оп­ти­че­ские ка­на­лы утеч­ки ин­фор­ма­ции | |
| 4 | Ра­дио­элек­трон­ные ка­на­лы утеч­ки ин­фор­ма­ции | |
| 5 | Ма­те­ри­аль­но-ве­ще­ст­вен­ные ка­на­лы утеч­ки ин­фор­ма­ции | |
| 6 | Каналы утечки акустической (речевой) информации | |
| 7 | Закладные устройства | |
| **Семинарские занятия** | | | **14** | 2 |
| **Практическая работа** | | | **8** | 3 |
| 1 | Определение ва­ри­ан­тов утеч­ки ин­фор­ма­ции по оп­ти­че­ским ка­на­лам для ти­по­вых кон­тро­ли­руе­мых зон ор­га­ни­за­ции. | |
| 2 | Изучение ха­рак­те­ри­сти­к элек­трических ка­на­лов утеч­ки ин­фор­ма­ции | |
| 3 | Изучение характеристик электромагнитных каналов утечки информации | |
|  | 4 | Изучение характеристик акустического канала утечки информации | |
| **Тема 1.5** **Методы добывания информации** | **Содержание** | | | **22** | 3 |
| 1 | Ор­га­ны до­бы­ва­ния ин­фор­ма­ции. Классификация технических разведок и методы противодействия им. | |  |
| 2 | Тех­но­ло­гия до­бы­ва­ния ин­фор­ма­ции. | |
| 3 | Спо­со­бы не­санк­цио­ни­ро­ван­но­го дос­ту­па к ис­точ­ни­кам ин­фор­ма­ции | |
| 4 | Спо­со­бы и сред­ст­ва до­бы­ва­ния ин­фор­ма­ции тех­ни­че­ски­ми сред­ст­ва­ми | |
| 5 | Способы и средства перехвата сигналов. | |
| 6 | Способы и средства подслушивания акустических сигналов. | |
| **Семинарские занятия** | | | **12** |  |
| **Практическая работа** | | | **10** | 2 |
| 1 | Изучение характеристик наземных средств дистанционного съема информации с носителей | |
| 2 | Изучение основных характеристик средств наблюдения | |
| 3 | Анализ современных средств перехвата сигналов | |
| 4 | Изучение особенностей и основных характеристик средств перехвата сигналов | |
| **Тема 1.6. Методы, способы и средства технической защиты информации**. | **Содержание** | | | **48** | 2 |
| 1 | Обеспечение безопасности объектов | |  |
| 2 | Способы и средства защиты информации от утечки по оптическим каналам | |
| 3 | Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки | |
| 4 | Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам | |
| 5 | Методы и средства выявления электронных устройств негласного получения информации | |
| 6 | Способы предотвращения утечки информации по материально-вещественному каналу | |
| 7 | Средства обеспечения информационной безопасности в компьютерных системах | |
| **Семинарские занятия** | | | **24** | 2 |
| **Практическая работа** | | | **24** | 3 |
| 1 | Построение системы периметровой охраны | |
| 2 | Изучение систем защиты территории и помещения | |
| 3 | Изучение характеристик средства защиты информации от утечки по оптическим каналам | |
| 4 | Сетевые помехоподавляющие пассивные фильтры низких и высоких частот | |
| 5 | Сетевые пассивные полосно-заграждающие и полосно-пропускающие фильтры | |
| 6 | Анализ способов технического закрытия от утечки речевой информации | |
| 7 | Изучение сущности и параметров звукоизоляции | |
| 8 | Изучение принципов работы и основных характеристик обнаружителей электромагнитного поля | |
| 9 | Изучение средств обеспечения информационной безопасности в компьютерных системах | |
| 10 | Изучение принципа работы локатора нелинейности | |
| 11 | Изучение аппаратуры и способов активной защиты помещений от утечек | |
| 12 | Изучение защиты электронных устройств и объектов от побочных электромагнитных излучений | |
| **Тема 1.7**. **Мероприятия по выявлению каналов утечки информации** | **Содержание** | | | **6** | 3 |
| 1 | Специальные проверки. | |  |
| 2 | Специальные обследования. | |
| 3 | Специальные исследования. | |
| **Семинарские занятия** | | | **2** | 3 |
| **Практическая работа** | | | **4** | 3 |
| 1 | Изучение типового набора операций при проведении технических проверок | |  |
| 2 | Оценка вероятного противника и выполнение поисковых мероприятий при специальном обследовании | |
| **Тема 1.8. Организация технической защиты информации** | **Содержание** | | | **6** | 2 |
| 1 | Порядок организации ТЗИ | |  |
| 2 | Порядок организации и проведения аттестации объекта информатизации | |
| **Семинарские занятия** | | | **4** | 2 |
| **Практическая работа** | | | **2** | 3 |
| 1 | Изучение порядка организации ТЗИ объекта информатизации | |  |
| **Тема 1.9. Основы проектирования защиты объектов информатизации** | **Содержание** | | | **18** | 3 |
| 1 | Моделировании объектов защиты информации. | |  |  |
| 2 | Проектирование защиты информации | |
| 3 | Определение требований к защите информации | |
| 4 | Оценивание защищенности информации от утечки по возможным ТКУИ | |
| 5 | Выбор средств защиты информации | |
| 6 | Изучение методики принятия решения на защиту от утечки информации в организации | |
| **Семинарские занятия** | | | **8** | 3 |
| **Практическая работа** | | | **10** | 3 |
| 1 | Оценка возможностей злоумышленника | |
| 2 | Оценка своей организации как возможного источника информации для противника | |
| 3 | Моделирование угроз безопасности информации | |
| 4 | Оценивание защищенности информации от утечки по возможным ТКУИ | |
|  | 5 | Построение системы защиты | |  |  |
| **Самостоятельная работа при изучении раздела ПМ 3**   1. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). 2. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов и подготовка к их защите 3. Составление опорного конспекта. 4. Составление тезисов. 5. Работа с электронными информационными ресурсами и ресурсами Internet 6. Решение вариативных задач и упражнений. | | | | **80** |  |
| **Примерная тематика внеаудиторной самостоятельной работы**   1. Подготовка презентации при выполнении практических работ. 2. Составление терминологического словаря по модулю. 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**   * решение аналитических задач; * освоение методики выявления технических каналов утечки информации на примерах организаций; * установка систем и средств защиты информации защищаемых объектов; * освоение методики выявления возможных угроз информационной безопасности объектов защиты. | | | | **18** |  |
| **Виды работ по практике** **по профилю специальности**   * решение аналитических задач; * выявление технических каналов утечки информации на примерах организаций; * оценивание защищенности информации; * эксплуатация систем и средств защиты информации защищаемых объектов; * применения технических средств защиты информации; * выявления возможных угроз информационной безопасности объектов защиты; * оснащение режимных объектов на примере организаций | | | | **54** |  |
| **Раздел 2 ПМ.03 Программно-аппаратные и технические средства защиты информации** |  | | | **200** |  |
| **МДК.03.02.** **Организация работы персонала с конфиденциальной информацией** |  | | | **200** |  |
| **Раздел 1. Защита информации в операционных системах, вычислительных сетях и базах данных** |  | | |  |  |
| **Тема 1.1. Общие принципы построения подсистемы защиты компьютерной системы** | **Содержание** | | | **10** | 2 |
| 1 | Фрагментарный и комплексный подходы к построению защищенных систем. | |  |  |
| 2 | Адекватная политика безопасности, этапы ее определения и поддержания. | |
| 3 | Перечень основных функций подсистемы безопасности защищенной компьютерной системы. | |
| **Семинарские занятия** | | | **2** | 2 |
| **Практическая работа** | | | **8** | 2 |
| 1 | | Защита информации в компьютерной системы от случайных угроз. |
| 2 | | Создание и управление учетными записями пользователей. |
| 3 | | Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS. |
| 4 | | Повышение безопасности информации встроенными средствами шифрования операционной системы. |
| **Тема 1.2. Разграничение доступа** | **Содержание** | | | **22** | 3 |
| 1 | Основные требования к подсистеме разграничения доступа. | |  | 3 |
| 2 | Полномочное разграничение доступа, проблемы его реализации в операционных системах | |
| 3 | Объекты доступа Windows. | |
| 4 | Дескриптор защиты объекта | |
| 5 | Специфичные и стандартные методы доступа к объектам | |
| 6 | Субъекты доступа Windows | |
| 7 | Объекты, субъекты, методы и права доступа в UNIX. | |
| 8 | Порядок проверки прав доступа субъекта к объекту. Механизм SUID/SGID | |  |  |
| **Семинарские занятия** | | | **14** | 3 |
| **Практическая работа** | | | **8** |  |
| 1 | Консоль управления mmc. Разграничение доступа в Windows. | |
| 2 | Конфигурирование полномочий доступа к файловой системе Windows. | |
| 3 | Изучение файловой системы в UNIX. Стандартный вход и стандартный выход. Перенаправление входа и выхода. | |
| 4 | Права доступа к файлам в операционной системе UNIX. | |
| **Тема 1.3. Аутентификация** | **Содержание** | | | **20** | 2 |
| 1 | Парольная аутентификация, хранение эталонных образов паролей. Методы подбора паролей. | |  |
| 2 | Средства и методы защиты от подбора и компрометации паролей. | |
| 3 | Аутентификация с использованием внешних носителей информации. Биометрическая аутентификация. | |
| 4 | Архитектура подсистемы аутентификации Windows. Параметры аутентификации | |
| 5 | Аутентификация в UNIX.  Архитектура PAM. | |
| **Семинарские занятия** | | | **10** | 2 |
| **Практическая работа** | | | **10** | 3 |
| 1 | Аутентификация в Windows. | |  |
| 2 | Аутентификация в UNIX. | |
| 3 | Аутентификация в базах данных. | |
| 4 | Механизмы СУБД для разграничения доступа в базах данных. | |
| **Тема 1.4. Аудит** | **Содержание** | | | **30** | 3 |
| 1 | Необходимость аудита в защищенной компьютерной системе. | |  |
| 2 | Требования к подсистеме аудита. | |
| 3 | Политика аудита, требования к адекватной политике аудита. | |
| 4 | Журнал аудита. | |
| 5 | Политика аудита, категории событий аудита. | |
| 6 | Порядок регистрации обращений пользователей к объектам операционной системы. | |
| **Семинарские занятия** | | | **18** | 3 |
| **Практическая работа** | | | **12** | 3 |
| 1 | Аудит в Windows. Планирование и настройка политики аудита ресурсов и событий. | |
| 2 | Настройка аудита объектов Windows XP Professional. | |
| 3 | Управление журналом безопасности. | |
| 4 | Аудит в Linux: Аудит доступа к файлам в Linux. | |
| 5 | Аудит в Linux: Аудит системных событий в Linux. | |
| **Раздел 2.**  **Введение в защиту программ и данных** |  | | |  |  |
| **Тема 2.1. Защита программ и данных от несанкционированного копирования** | **Содержание** | | | **22** | 2 |
| 1 | Программа. Три основных этапа анализа программы. | |  |
| 2 | Метод экспериментов. Статический метод. | |
| 3 | Проблемы при практической реализации алгоритмов дизассемблирования. | |
| 4 | Особенности анализа некоторых видов программ (оверлейные программы, консольные приложения, графические программы под управлением Windows). | |
| **Семинарские занятия** | | | **16** | 2 |
| **Практическая работа** | | | **6** | 3 |
| 1 | Знакомство с системами защиты программ и данных от несанкционированного копирования. | |
| 2 | Способы преодоления защиты от несанкционированного копирования. | |
| **Тема 2.2**  **Компьютерные вирусы** | **Содержание** | | | **30** | 3 |
| 1 | Понятие вируса. Классы вирусов. | |  |
| 2 | Теории происхождения компьютерных вирусов. | |
| 3 | Механизмы распространения вирусов. | |
| 4 | Этапы исполнения компьютерного вируса. | |
| 5 | Признаки заражения компьютера вирусами. | |
| 6 | Борьба с компьютерными вирусами. | |
| 7 | Понятие антивируса. | |
| 8 | Классификация и сравнительная характеристика антивирусных программ. | |
| 9 | Создание компьютерного вируса. | |
| **Семинарские занятия** | | | **16** | 3 |
| **Практическая работа** | | | **14** | 3 |
| 1 | Основные признаки присутствия на ПК вредоносных программ. | |
| 2 | Принципы диагностики антивирусной защиты. | |
| 3 | Настройка работы брандмауэра. | |
| 4 | Установка и настройка антивирусных программ. | |
| 5 | Установка и настройка FIREWALL. | |
| 6 | Архивация и восстановление данных. | |
| 7 | Настройка параметров безопасности подключения к Интернет. | |
| 8 | Работа с командной строкой. Сетевая активность. | |
| **Самостоятельная работа при изучении МДК 03.02.**   1. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). 2. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов и подготовка к их защите. 3. Составление опорного конспекта. 4. Составление тезисов. 5. Работа с электронными информационными ресурсами и ресурсами Internet 6. Решение вариативных задач и упражнений. 7. Работа с компьютерными программами. | | | | **66** |  |
| **Примерная тематика внеаудиторной самостоятельной работы**   1. Составление терминологического словаря по теме «Основные команды для работы с файлами и каталогами в операционной системе Linux». 2. Создание презентаций по теме «Сравнительный анализ схемы разграничения доступа в операционных системах Windows и Unix», «Сравнительный анализ схемы аутентификации в операционных системах Windows и Unix». 3. Подготовка доклада по теме «Идентификация и аутентификация в базах данных». 4. Подготовка рефератов на темы: «Инсталляция различных версий Linux», «Сравнительная характеристика операционных систем (MS-DOS, Windows, Unix, Linux и MacOS)». 5. Конспекты по темам: «Ядро Linux», «Создание системных оболочек под Linux», «Аудит и восстановление паролей в Windows». 6. Доклад на тему: «Настройка безопасной виртуальной сети Linux». 7. Чтение дополнительной литературы. 8. Ответы на контрольные вопросы. 9. Составление тестовых заданий по темам семинарских занятий. | | | |  |  |
| **Виды работ по учебной практике**   * решение аналитических задач; * оценивание защищенности информации в АС; * установка систем и средств программно-аппаратной защиты информации; * тестирование программно-аппаратных средств защиты информации; * освоение методики выявления возможных угроз информационной безопасности автоматизированных систем; | | | | **18** |  |
| **Виды работ по практике** **по профилю специальности**   * решение аналитических задач; * выявление технических каналов утечки информации на примерах организаций; * оценивание защищенности информации; * эксплуатация систем и средств программно-аппаратной защиты информации; * применение программно-аппаратных средств защиты информации; * выявления возможных угроз информационной безопасности объектов защиты; * оснащение режимных объектов на примере организаций | | | | **54** |  |

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 кабинета «Информационной безопасности», «Вычислительной техники» и лаборатории технических средств защиты информации, программно-аппаратных средств защиты информации;

Оборудование учебных кабинетов и лабораторий:

посадочные места по количеству обучающихся, рабочее место преподавателя; рабочие программы по МДК, методическая литература; комплект учебной литературы по дисциплине; электронные учебные издания; электронные симуляторы; 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:**

**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. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И.К.Корнеев, Е.А. Степанов.- М.:Проспект,2011.-336 с.
5. Защита информации в персональном компьютере: учебное пособие/ Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – М.: ФОРУМ, 2012, 368 с.
6. Зегжда Д.П., Ивашко A.M. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2009.
7. М.Купер Анализ типовых нарушений безопасности в сетях – М.: Вильямс, 2010.
8. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студентов учреждений высшего профессионального образования. – Академия ИЦ, 2012. – 331 с.

**Интернет ресурсы:**

* www.bnti.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/)

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

Программа профессионального модуля ПМ.03 Программно-аппаратные и технические средства защиты информации реализуется в течение 2-х семестров.

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.01 Участие в планировании и организации работ по обеспечению защиты объекта**,** ПМ.02 «Организация и технология работы с конфиденциальными документами».

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

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

**4.4. Кадровое обеспечение образовательного процесса**

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарному курсу**:** наличие высшего профессионального образования, соответствующего профилю модуля и специальности 090905 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 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах | - соблюдение методики применения программно-аппаратных и технических средств защиты информации;  - соответствие выбранных программно-аппаратных и технических средств ЗИ степени конфиденциальности 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**:  Комплексны дифференцированный зачет по разделам профессионального модуля.  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 |
| 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;  - соблюдение алгоритма фиксирования отказов средств защиты информации. |
| ПК 3.4 Выявлять и анализировать возможные угрозы информационной безопасности объектов. | - соответствие построенной модели угроз наиболее вероятным реальным угрозам;  - грамотный анализ соответствия (или несоответствия) примененных методов защиты объекта реальным угрозам информационной безопасности объектов; |

**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 экзамен;  - положительные отзывы руководителей производственной практики от предприятий-баз практики. |
| ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. | - 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. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей). | - рейтинг участия во внеаудиторных мероприятиях патриотической направленности; | Интерпретация результатов наблюдений за деятельностью студента в процессе освоения программы профессионального модуля. |
| ОК 11. 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 12. 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; |
| ОК13. 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. |