

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО на базе основного общего образования с одновременным получением среднего общего образования. Программа разработана с учетом требований ФГОС среднего общего образования (приказ Минобрнауки России от 17.05.2012г. № 413) и требованиями ФГОС среднего профессионального образования по специальности 10.02.01 «Организация и технология защиты информации», утвержден приказом Министерством образования и науки Российской Федерации от 28 июля 2014г. №805 зарегистрирован Министерством юстиции 21 августа 2014г. №33750, укрупненная группа 10.00.00 информационная безопасность, утверждена приказом Минобрнауки России от 29 октября 2013г. №1199.

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

В результате освоения ПМ.02 обучающийся должен обладать **общими компетенциями, включающими в себя способность:**

- 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.

В результате освоения ПМ.02 обучающийся должен обладать

профессиональными компетенциями, соответствующими основным видам профессиональной деятельности:

ПК 2.1. Участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации.

ПК 2.2. Участвовать в организации и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации.

ПК 2.3. Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации.

ПК 2.4. Организовывать архивное хранение конфиденциальных документов.

ПК 2.5. Оформлять документацию по оперативному управлению средствами защиты информации и персоналом.

ПК 2.6. Вести учет работ и объектов, подлежащих защите.

ПК 2.7. Подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации.

ПК 2.8. Документировать ход и результаты служебного расследования.

ПК 2.9. Использовать нормативные правовые акты, нормативно-методические документы по защите информации.

В результате изучения профессионального модуля обучающийся должен:

иметь практический опыт:

- ведения учета и оформления бумажных и машинных носителей конфиденциальной информации;
- работы с информационными системами электронного документооборота;

уметь:

- использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;
- документировать ход и результаты служебного расследования;
- определять состав документируемой конфиденциальной информации;
- подготавливать, издавать и учитывать конфиденциальные документы;
- составлять номенклатуру конфиденциальных дел;
- формировать и оформлять конфиденциальные дела;
- организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники;

- использовать системы электронного документооборота;
- *проводить информационные обследования, выявлять значимые угрозы, анализировать и оценивать риски, применять различные защитные механизмы;*
- *разрабатывать нормативно-методические и организационно-распорядительные документы, необходимые для реализации выбранных технологий защиты;*
- *определение подходов к оценке характеристик и выбору необходимых программно-аппаратных и программных средств защиты информационных ресурсов, основы поиска и использования оперативной информации об угрозах и средствах защиты, другой актуальной информации по безопасности автоматизированных систем;*
- *контролировать и анализировать эффективность применения конкретных мер и средств защиты информации;*
- *грамотно выстроить на предприятии политику безопасности.*

знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы защиты конфиденциальной информации по видам тайны;
- порядок лицензирования деятельности по технической защите конфиденциальной информации;
- правовые основы деятельности подразделений защиты информации;
- правовую основу допуска и доступа персонала к защищаемым сведениям;
- правовое регулирование взаимоотношений администрации и персонала в области защиты информации;
- систему правовой ответственности за утечку информации и утрату носителей информации;
- правовые нормы в области защиты интеллектуальной собственности;
- порядок отнесения информации к разряду конфиденциальной информации;
- порядок разработки, учета, хранения, размножения и уничтожения конфиденциальных документов;
- организацию конфиденциального документооборота;
- технологию работы с конфиденциальными документами;
- организацию электронного документооборота;
- *методы защиты информации;*
- *правовые вопросы защиты информации;*

- теории построения защищенных систем;
- организацию работы подразделений информационной безопасности;
- основы построения комплексных систем защиты, обеспечивающих рациональное распределение функций и эффективное взаимодействие по вопросам защиты информации сотрудников всех структурных подразделений организации;
- эксплуатационные характеристики основных средств защиты информации (средства предотвращения несанкционированного доступа, криптографическая защита, межсетевые экраны, средства анализа защищенности и обнаружения атак);
- проблемы безопасности в Internet/intranet, уязвимости распространенных операционных систем, СУБД и приложений, сетевых протоколов и служб, атаки в IP-сетях, типовые приемы проникновения в корпоративные сети, реализуемые за счет использования данных уязвимостей, и популярные у нарушителей инструменты взлома;
- основы поиска и использования оперативной информации о новых уязвимостях в системном и прикладном программном обеспечении.