АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ
ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средствах защиты

Область применения программы:

Рабочая программа профессионального модуля (далее рабочая программа) является частью программы подготовки специалистов среднего звена. Разработана в соответствии с ФГОС СПО специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в части освоения основного вида деятельности: защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты и соответствующих профессиональных компетенций:

ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.

ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.

ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании.

Показатели освоения профессионального модуля:

Результатом освоения общепрофессиональной дисциплины является овладение профессиональными (ПК) и общими (ОК) компетенциями:

ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.

ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.

ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в

соответствии с предъявляемыми требованиями.

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями в ходе освоения профессионального модуля обучающийся должен:

иметь практический опыт:

– применения программно-аппаратных средств обеспечения информационной безопасности;

– диагностики, устранение отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности;

– мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;

– обеспечение учета, обработки, хранения и передачи конфиденциальной информации;

– решение частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;

– применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами.

уметь:

– применять программно-аппаратные средства обеспечения информационной безопасности;

– диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;

– оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;

– участвовать в обеспечение учета, обработки, хранения и передачи конфиденциальной информации;

– решать частые технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;

– использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;

– применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

знать:

– методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;

– особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;

– типовые модели управления доступом;

– типовые средства, методы и протоколы идентификации, аутентификации и авторизации;

– типовые средства и методы ведения аудита и обнаружение вторжений;

– типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;

– основные понятия криптографии и типовые криптографические методы защиты информации