АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и соответствующие ему общие компетенции, и профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Общие компетенции
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 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК.11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.1.2. Перечень профессиональных компетенций

Код	Профессиональные компетенции
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.1.3. В результате освоения профессионального модуля обучающийся должен:

иметь практический опыт	− установки и настройки программных средств защиты информации (06.032 A/01.5) в автоматизированной системе; − обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; − тестирования функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации (06.032 A/01.5); − решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; − применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; − учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности, *информирование персонала об угрозах безопасности*

	информации (06.033 А/02.5) − работы с подсистемами регистрации событий; − выявления событий и инцидентов безопасности в автоматизированной системе; − *применения технологии фильтрации различных видов трафика,* − *осуществлять фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.**
уметь	− устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; − устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями (06.032 А/01.5); − диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации*, проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах* (06.032 А/01.5); − применять программные и программно-аппаратные средства для защиты информации в базах данных; − проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; − применять математический аппарат для выполнения криптографических преобразований; − использовать типовые программные криптографические средства, в том числе электронную подпись (06.033 А/03.5); − применять средства гарантированного уничтожения информации; − осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; − *оформлять эксплуатационную документацию*

	программно-аппаратных средств защиты информации (06.032 А/01.5); − *определять цели и задачи в изучении проекта;* − *разрабатывать политику информационной безопасности на основе самостоятельной классификации объектов защиты;* − *осуществлять установку, развёртывание, настройку и использованием DLP-систем.**
знать	- особенности и способы применения программных и программно-аппаратных средств защиты информации в автоматизированных системах (06.033 А/01.5), в том числе, в операционных системах, компьютерных сетях, базах данных; − методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; − типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации (06.033 А/01.5); − основные понятия криптографии и типовых криптографических методов и средств защиты информации; *общие принципы функционирования средств защиты информации, в том числе и криптографической защиты информации (*06.033 А/01.5), − особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; − типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа (06.033 А/01.5); − *теоретические основы корпоративной защиты информации от внутренних ИТ-угроз; методику проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его; современные стандарты и средства корпоративной защиты.**

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 798 часа,

Из них на освоение МДК 480 часов,

самостоятельная работа 18 часов,

промежуточная аттестация 48 часов, в том числе экзамен по модулю 12 часов,

на практики 252 часа, в том числе учебную 108 часа,

и производственную (по профилю специальности) 144 часа.