

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПМ.02 «Организация и технология работы с конфиденциальными документами»

1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) – является частью ППССЗ в соответствии с ФГОС по специальности 10.02.01 «Организация и технология защиты информации» в части освоения основного вида профессиональной деятельности (ВПД): «Организация и технология работы с конфиденциальными документами» и соответствующих профессиональных компетенций (ПК):

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.

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

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями учащийся в ходе освоения профессионального модуля 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 сравнительный анализ СЭД;*
- *работать с электронным архивом;*

- *разрабатывать модели основных бизнес-процессов в области документооборота;*
- *составлять проект технического задания;*
- *оформлять техническое задание;*
- *разрабатывать локальные акты предприятия в области организации защиты коммерческой тайны;*
- *разрабатывать локальные акты предприятия в области защиты персональных данных;*
- *проводить аудит состояния информационной безопасности предприятия*

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;*
- *технологии работы с конфиденциальными документами;*
- *организацию электронного документооборота;*
- *подходы к автоматизации документооборота в организации и требования к СЭД;*
- *тенденции рынка специализированного программного обеспечения в области автоматизации документооборота;*
- *критерии выбора СЭД;*
- *процессный подход к описанию документооборота организации и принципы рационализации управления документооборотом;*
- *методологию описания бизнес-процессов;*
- *жизненный цикл СЭД;*
- *методику внедрения СЭД;*
- *структуру технического задания;*
- *правила оформления технического задания;*
- *правила согласования и утверждения технического задания,*
- *порядок организации защиты коммерческой тайны на предприятии;*
- *порядок организации защиты персональных данных на предприятии;*
- *структуру политики безопасности предприятия;*
- *порядок проведения аудита информационной безопасности предприятия.*

1.3. Планируемое количество часов на освоение программы ПМ.02:

всего **870** часов, в том числе:

максимальная учебная нагрузка - **582** часов, включая:

обязательную аудиторную учебную нагрузку **388** часа;

самостоятельную работу - **194** часов;

учебная и производственная практики - **288** часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности «Планирование и организация логистического процесса в организациях (в подразделениях) различных сфер деятельности», в том числе профессиональными (ПК) и общими (ОК) компетенциями.

Код	Наименование результата обучения
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.
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.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Формы и методы контроля и оценки результатов обучения должны позволять проверять у учащихся не только получение профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
Участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации	Подготовка организационных и распорядительных документов	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов. Экзамен по ПМ.
Участвовать в организации и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации	Подготовка локальных нормативных актов	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов. Экзамен по ПМ.
Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации.	Подготовка локальных нормативных актов, настройка информационных баз	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики Экзамен по ПМ.

<p>Организовывать архивное хранение конфиденциальных документов.</p>	<p>Подготовка локальных нормативных актов, настройка информационных баз</p>	<p>Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики</p> <p>Экзамен по ПМ.</p>
<p>Оформлять документацию по оперативному управлению средствами защиты информации и персоналом.</p>	<p>Оформление журналов и отчетных документов</p>	<p>Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов</p> <p>Экзамен по ПМ.</p>
<p>Вести учет работ и объектов, подлежащих защите</p>	<p>Подготовка и заполнение журналов</p>	<p>Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов</p> <p>Экзамен по ПМ.</p>
<p>Подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации.</p>	<p>Оформление отчетной документации</p>	<p>Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов</p> <p>Экзамен по ПМ.</p>

Документировать ход и результаты служебного расследования.	Подготовка организационно-распорядительных и отчетных документов	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Экзамен по ПМ.
Использовать нормативные правовые акты, нормативно-методические документы по защите информации.	Разработка локальных актов предприятия в области организации защиты коммерческой тайны и персональных данных	Экспертная оценка разработанных материалов Экзамен по ПМ.

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности	проявление интереса к будущей профессии в процессе теоретического обучения, производственной практики	Проверка качества выполнения практических работ, проверка отчетной документации по практике
Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	выбор и применение эффективных методов и способов решения профессиональных задач в профессиональной области; собственная оценка эффективности и качества выполнения заданий.	Анализ результатов практических работ
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	решение стандартных и нестандартных профессиональных задач	Анализ результатов практических работ
Осуществлять поиск и использование информации, необходимой для эффективного	эффективный поиск необходимой информации;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
выполнения профессиональных задач, профессионального и личностного развития	использование различных источников, включая электронные	освоения образовательной программы
Использовать информационно-коммуникационные технологии в профессиональной деятельности	работа с различными прикладными программами	Анализ результатов практических работ
Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями	взаимодействие с обучающимися, преподавателями в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий	работа в группах, выполнение групповых заданий	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	взаимодействие с обучающимися, преподавателями в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Ориентироваться в условиях частой смены технологий в профессиональной деятельности	Анализ инноваций в сфере защиты информации; работа с различными прикладными программами	Анализ результатов практических работ
Применять математический аппарат для решения профессиональных задач.	Применение математических расчетов в ходе решения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Анализ результатов практических работ
Оценивать значимость документов, применяемых в профессиональной деятельности.	работа с различными источниками информации нормативно-правой информации	Анализ результатов практических работ
Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих	работа с различными источниками информации	Анализ результатов практических работ

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
информационную безопасность.	нормативно-правой информации	

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПМ.03 «Программно-аппаратные и технические средства защиты информации»

1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) – является частью ППССЗ в соответствии с ФГОС по специальности 10.02.01 «Организация и технология защиты информации» в части освоения основного вида профессиональной деятельности (ВПД): «Программно-аппаратные и технические средства защиты информации» и соответствующих профессиональных компетенций.

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

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями учащийся 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;
- применять на практике навыки монтажа кабельных сетей;
- работать с сетевым оборудованием и сетевым программным обеспечением;
- конфигурировать оборудование для организации статической маршрутизации в локальных компьютерных сетях;
- производить настройку соединений на канальном уровне, создавать и управлять виртуальными локальными сетями;
- конфигурировать протоколы динамической маршрутизации в локальных компьютерных сетях (RIP, OSPF);
- настраивать агрегированные каналы и обеспечивать отказоустойчивость канальной подсистемы;
- проводить анализ безопасности оборудования в локальной сети,
- применять на практике алгоритмы шифрования секретным ключом;
- проводить анализ криптостойкости алгоритмов и протоколов;
- создавать программы, реализующие алгоритмы и протоколы защищенной передачи данных;
- конструировать крипто-стойкие алгоритмы и протоколы;
- проводить анализ данных на наличие скрытой информации,
- *настраивать ALD домен на операционной системе AstraLinuxSE*
- *настраивать политики безопасности, создавать пользователей при использовании ALD домена AstraLinuxSE;*

- осуществлять установку системы обнаружения и предотвращения вторжения *IDS VipNet*;
- осуществлять имитацию атаки с помощью *KaliLinux*;
- осуществлять настройку веб-интерфейса для системы обнаружения и предотвращения вторжения *IDS VipNet*;
- создавать правила для *IDS VipNet*;
- создавать сертификаты для защиты данных при передаче через глобальную сеть;
- применять сертификаты для защиты данных при передаче через глобальную сеть;
- создавать и модифицировать защищенную сеть;
- осуществлять настройку политик безопасности для защищенной сети;
- организовывать и модифицировать межсетевое взаимодействие;
- добавлять дополнительные рабочие места в защищенную сеть;
- осуществлять установку и настройку компонентов *DLP-системы Infowatch*;
- осуществлять установку клиента, настройку периметра компании, добавлять пользователей и компьютеров в домен;
- осуществлять контроль документов на сетевых ресурсах;
- создавать правила *Device monitor*;
- управлять ролями в *Traffic monitor*;
- создавать и настраивать политики безопасности в *Traffic monitor*;
- использовать регулярные выражения при создании политик безопасности в *Traffic monitor*;
- осуществлять работу с отчетами в *Traffic Monitor*
- выбирать аппаратную конфигурацию персонального компьютера, сервера и периферийного оборудования, оптимальную для решения задач пользователя;
- собирать и разбирать на основные компоненты (блоки) персональные компьютеры, серверы, периферийные устройства, оборудование и компьютерную оргтехнику;
- подключать кабельную систему персональных компьютеров, серверов, периферийных устройств, оборудования и компьютерной оргтехники;
- настраивать параметры функционирования аппаратного обеспечения;
- диагностировать работоспособность аппаратного обеспечения;
- устранять неполадки и сбои в работе аппаратного обеспечения;
- заменять неработоспособные компоненты аппаратного обеспечения на аналогичные или совместимые;
- заменять расходные материалы и быстро изнашиваемые части аппаратного обеспечения на аналогичные или совместимые;
- направлять аппаратное обеспечение на ремонт в специализированные сервисные центры;
- вести отчетную и техническую документацию;
- осуществлять приём, выдачу и рассылку документов и сведений, связанных с организацией и проведением закупок;
- планировать закупки;
- разрабатывать извещение и документацию по закупкам;

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 правовых актов.
- основы сетей передачи данных;
- основы статической маршрутизации;
- структуру и назначение универсального идентификатора ресурсов;
- технологию организации работы глобальных компьютерных сетей;
- основные сетевые информационные службы;
- основы безопасности компьютерных сетей,
- *принципы использования систем обнаружения вторжения;*
- *понятие протокола https;*
- основные понятия, определения, основные алгоритмы шифрования с секретным ключом;
- основные понятия, определения, модель передачи защищенных сообщений с открытым ключом шифрования;
- основные понятия, определения и алгоритмы стеганографии;
- основные принципы анализа криптографических систем;
- *виды сертификатов сайтов для защиты данных при передаче информации через глобальную сеть;*
- *общую характеристику и принципы функционирования dlp-системы Infowatch;*
- *виды политик, способы их создания в Traffic monitor;*
- *принципы построения регулярных выражений для создания политик;*
- *виды правил и способы создания правил в Device monitor;*
- *ложные срабатывания политик;*
- *принципы мониторинга событий информационной безопасности в DLP-системе Infowatch;*
- *классификацию видов и архитектуру персональных компьютеров и серверов;*
- *устройство персонального компьютера и серверов, их основные блоки, функции и технические характеристики;*
- *назначение разделов и основные установки BIOS персонального компьютера и серверов;*
- *виды и назначение периферийных устройств, их устройство и принцип действия, интерфейсы подключения и правила эксплуатации;*

- нормативные документы по установке, эксплуатации и охране труда при работе с персональным компьютером, серверами, периферийным оборудованием и компьютерной оргтехникой;
- методики диагностики конфликтов и неисправностей компонентов аппаратного обеспечения;
- способы устранения неполадок и сбоев аппаратного обеспечения;
- методы замены неработоспособных компонентов аппаратного обеспечения;
- состав процедуры гарантийного ремонта аппаратного обеспечения в специализированных сервисных центрах
- положения федерального законодательства о контрактной системе в сфере закупок и иных сопутствующих нормативных правовых актов;
- основные этапы проведения закупки, требований законодательства к организации и проведению процедур определения поставщика при применении различных способов закупки;
-

1.3. Планируемое количество часов на освоение программы ПМ.03:

всего **1256** часов, в том числе:

максимальная учебная нагрузка - **952** часов, включая:

обязательную аудиторную учебную нагрузку **634** часов;

самостоятельную работу - **317** часов;

учебная практика - **36** часов;

производственная практика **288** часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности «Программно-аппаратные и технические средства 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
ПК 3.5.	<i>Применять DLP-системы в профессиональной деятельности</i>
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 личного 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 личного 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.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

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	
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, Часов	в т.ч., курсовая работа (проект), часов			
1	2	3	4	5	6	7	8	9	10	
ПК 3.1. – ПК 3.4.	Раздел 1. Технические методы и средства, технологии защиты информации	153	102	50		51				
ПК 3.1. – ПК 3.5.	Раздел 2. Программно-аппаратные средства защиты информации	295	196	130	20	98				
ПК 3.1. – ПК 3.5.	Раздел 3. Компьютерные сети	144	96	64		48				
ПК 3.1. – ПК 3.5.	Раздел 4. Основы криптографической защиты данных	84	56	46		28				
ПК 3.1. – ПК 3.5.	Раздел 5. Эксплуатация аппаратного и	138	92	60		46				

	программного обеспечения								
ПК 3.1. – ПК 3.5.	Раздел 6. Организация закупки оборудования и программного обеспечения	138	92	52		46			
ПК 3.1. – ПК 3.5.	Учебная практика, производственная практика, часов	324						36	288
	Всего:	1276	634	402	20	317		36	288

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы профессионального модуля требует наличия лаборатории технических средств защиты информации.

Оборудование лаборатории технических средств защиты информации:

Технические средства обучения:

- компьютеры с лицензионным программным обеспечением на каждом посадочном месте обучающихся и на рабочем месте преподавателя.

Оборудование полигона подразделения защиты информации:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-наглядных пособий, в т.ч. на электронных носителях.

Оборудование кабинета информационной безопасности:

- рабочие столы и стулья по количеству обучающихся;
- компьютер с лицензионным программным обеспечением и мультимедиапроектор, экран.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Формы и методы контроля и оценки результатов обучения должны позволять проверять у учащихся не только получение профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

