Министерство образования Ставропольского края
Государственное бюджетное профессиональное образовательное учреждение
«Пятигорский техникум торговли, технологий и сервиса»
(ГБПОУ ПТТТиС)

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ПРАКТИКИ

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация – техник по защите информации

2024 г.

СОДЕРЖАНИЕ

I. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1. Область применения программы учебной практики

Программа учебной практики является составной частью основной профессиональной образовательной программы (ОПОП СПО), разработанной по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» укрупненной группы 10.00.00 Информационная безопасность базовой подготовки. Учебная практика (по профилю специальности) проводятся при освоении студентами профессиональных компетенций в рамках профессиональных модулей.

1.2. Цели и задачи учебной практики

Учебная практика по специальности направлена на формирование у обучающихся умений, приобретение первоначального практического опыта в рамках освоения модулей ОПОП СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» укрупненной группы 10.00.00 Информационная безопасность базовой подготовки по виду профессиональной деятельности (ВПД):

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

- Защита информации в автоматизированных системах программными и программно-аппаратными средствами
- Защита информации техническими средствами

Выполнение работ по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин

Задачами учебной практики являются:

- эксплуатация автоматизированных (информационных) систем в защищенном исполнении
- защита информации в автоматизированных системах программными и программно-аппаратными средствами
- защита информации техническими средствами
- выполнение работ по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин
- закрепление и совершенствование первоначальных практических профессиональных умений обучающихся

Требования к результатам освоения программы учебной практики

В результате освоения программы учебной практики студент должен освоить основные виды профессиональной деятельности (ВПД) и соответствующие им общие и профессиональные компетенции.

по ВПД Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующих профессиональных компетенций (ПК).

Уметь	Осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; Организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; Осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; Производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы Настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; Обеспечивать работоспособность, обнаруживать и устранять неисправности *Выполнять настройку параметров работы программного обеспечения, включая системы управлениями базами данных* *Выполнять настройку параметров работы программного обеспечения, средства электронного документооборота* *Работать с программным обеспечением с соблюдением действующих требований по защите информации* *Контролировать процесс управления учетными записями пользователей СУБД* *Контролировать неизменность настроек средств защиты информации* *Работать в компьютерных сетях с соблюдением действующих требований по защите информации. Конфигурация и контроль корректности настройки программно-аппаратных средств защиты информации в компьютерных сетях* *Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных*

	сетях. *Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях* *Разрабатывать техническое задание на создание подсистем информационной безопасности автоматизированных систем* *Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности* *Работать с программным обеспечением с соблюдением действующих требований по защите информации* *Определять элементы кабельной системы, защищенные от НСД* *Определять оптимальность выбора аппаратных средств защиты информации* *Оценивать режимы выбора аппаратных средств защиты информации функционирования в компьютерных сетях* *Применять программно-аппаратных средств защиты информации в компьютерных сетях* *Настраивать правила фильтрации пакетов в компьютерных сетях* *Определять правила фильтрации пакетов в компьютерных сетях* *Настраивать правила фильтрации пакетов в компьютерных сетях с применение IPv4* *Оценивать оптимальности выбора аппаратных средств защиты информации* *Настраивать правила фильтрации пакетов и преобразование сетевых адресов* *Настраивать правила фильтрации пакетов с использованием NAT* *Настраивать правила фильтрации пакетов с использованием скрытого NAT* *Определять предложения по применению программных средств защиты информации в компьютерных сетях* *Определять предложения по применению программно-аппаратных средств защиты информации в компьютерных сетях* *Настраивать правила Spanning Tree Protocol*

	в компьютерных сетях *Определять правильность выбора аппаратно-программных средств защиты* *Вносить предложения по применению средств защиты информации в режиме функционирования* *Настраивать правила фильтрации пакетов в модели QoS* *Управлять количеством подключаемых к портам коммутатора пользователей* *Работать со снифферами* *Работать со стандартом IEEE 802.1AB-2009* *Фильтровать трафик между сетями или узлами сети* *Фильтровать трафик на основе MAC-адресов* *Работать с персональными межсетевыми экранами* *Работать с правилами фильтрования с использованием NAT* *Настраивать Сетевую Систему обнаружения вторжений* *Настраивать Сетевую Систему обнаружения вторжений, основанной на прикладных протоколах APIDS* *Блокировать атаки с помощью межсетевого экрана* *Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях*
Приобрести первоначальный практический опыт	Установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; Администрирования автоматизированных систем в защищенном исполнении; Эксплуатации компонентов систем защиты информации автоматизированных систем; Диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении *Настройки программно-аппаратных средств защиты информации, в тома числе антивирусной защиты в операционных системах по за-*

	данным шаблонам; *Инструктажа пользователей по порядку работы в операционных системах;* *Оформления эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах;* *Ввода в эксплуатацию программно-аппаратных средств за щиты информации в компьютерных сетях;* *Установки средств межсетевого экранирования в соответствии с действующими требованиями по защите информации* *Инструктажа пользователей по порядку безопасной работы в компьютерных сетях;* *Оформления эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях;* *Определения состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях.*

по ВПД Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Уметь	Устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; Устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; Диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; 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; Применять средства гарантированного уничтожения информации; Устанавливать, настраивать, применять программные и программно-аппаратные средства защиты 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; *Применять нормативные документы по противодействию технической разведке* *Применять нормативные документы для оценки уязвимости* *Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы* *Реализовывать правила разграничения доступа персонала к объектам доступа* *Настраивать параметры программного обеспечения системы защиты информации автоматизированной системы* *Работать с программой шифрования данных Kryptelite* *Классифицировать каналы утечки информации* *Реализовывать многоуровневую политику разграничения доступа средствами программно –аппаратного комплекса «Страж NT»* *Определять параметры работы с Windows Registry Recovery и Registry Explorer* *Выбирать методы защиты условно-бесплатного программного обеспечения* *Реализовывать защитные механизмы в приложениях свободно-распространяемого ПО* *Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации* *Устранять известные уязвимости автоматизированной системы, приводящих к возникновению угроз безопасности информации* *Разрабатывать предложения по совершенствованию системы управления защиты ин-*

	формации автоматизированной системы *Управлять рисками* *Применять механизмы и службы защиты* *Применять привилегии безопасности и доступа* *Применять протокол SSL* *Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем* *Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе* *Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации* *Обеспечивать безопасность рабочих станций и серверов* *Применять режимы работы блочных шифров, схемы кратного шифрования* *Проводить криптоанализ алгоритмов с открытым ключом* *Применять протоколы WPA, WEP для организации безопасного функционирования беспроводной сети* *Подбирать оборудование для реализации проекта беспроводной сети предприятия*
Приобрести первоначальный практический опыт	Установки, настройки программных средств защиты информации з автоматизированной системе; Обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; Тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ; Решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; Применения электронной подписи, симмет-

	ричных и асимметричных криптографических алгоритмов и средств шифрования данных; Учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; Работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе. *Определения правил и процедур управления системой защиты информации автоматизированной системы;* *Определения правил и процедур выявления инцидента;* *Определения правил и процедур реагирования на инциденты;* *Определения правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации.* *Определения правил и процедур управления системой защиты информации автоматизированной системы;* *Определения правил и процедур выявления инцидента;* *Определения правил и процедур реагирования на инциденты;* *Определения правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации.* *Выбора и обоснования критериев выбора эффективности функционирования защищенных автоматизированных систем;* *Проведения экспертизы состояния защищенности информации автоматизированных систем;* *Проведения предварительных испытаний системы защиты информации автоматизированной системы;* *Уточнения модели угроз безопасности информации автоматизированной системы.;* *Проведения занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне.*

По ВПД Защита информации техническими средствами:

Уметь	Применять технические средства для криптографической защиты информации конфиденциального характера; Применять технические средства для уничтожения информации и носителей информации; Применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; Применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; Применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; Применять инженерно-технические средства физической защиты объектов информатизации *Оценивать защищенность ограждающих конструкций помещения от утечки информации по акустическому каналу* *Оценивать защищенность ограждающих конструкций от утечки информации по виброакустическому каналу комплексом* *Проводить статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении.* *Проводить техническое обслуживание технических средств за щиты информации от утечки за счет побочных электромагнитных излучений и наводок* *Устранять выявленные неисправности технических средств за щиты информации от утечки за счет побочных электромагнитных излучений и наводок* *Проводить ремонт с привлечением производителей технических средств защиты информации* *Оценивать защищенность телефонных каналов* *Оценивать защищенность помещения от утечки информации по каналам акустоэлектрических преобразований технических средств*

	Обнаруживать ПЭМИ по электрической составляющей электромагнитного поля *Оценивать состояние трассы наблюдения* *Проводить испытания защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами* *Организовывать технический контроль эффективности мер защиты информации* *Проводить оценку разведдоступности* *Проводить комплекс работ по проверке возможности утечки информации по техническим каналам* *Проводить оценку защищенности объекта информатизации* *Разрабатывать проект системы видеонаблюдения для торговой организации* *Настраивать системы телевизионного наблюдения с учетом специфики деятельности организации* *Определять состав ССОИ для образовательной организации* *Испытывать на устойчивость технические средства охраны* *Разрабатывать проекты применения технических средств воздействия для образовательной организации* *Изготовлять технические средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок* *Отрабатывать конструкции технического средства защиты информации на технологичность с учетом стандартов ЕСТД* *Проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации* *Выполнять правила их эксплуатации средств защиты информации*
Приобрести первоначальный практический опыт	Установки, монтажа и настройки технических средств защиты информации; Технического обслуживания технических средств защиты информации; Применения основных типов технических средств защиты информации;

	Выявления технических каналов утечки информации; Участия в мониторинге эффективности технических средств защиты информации; Диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; Проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; Проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; Установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты. *Корректировки конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки, контроля и испытаний.* *Отработки конструкции средства защиты информации на технологичность с учетом стандартов ЕСТД;* *Заключения договоров с поставщиками комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности* *Сертификационных испытаний технических средств защиты информации от несанкционированного доступа на соответствие требованиям безопасности информации;* *Испытания опытного образца защищенного технического средства обработки информации на соответствие техническим условиям.*

В результате освоения программы учебной практики по виду профессиональной деятельности (ВПД): Выполнение работ по профессии рабочего 16199

Оператор электронно-вычислительных и вычислительных машин, обучающийся должен:

Уметь	выполнять требования техники безопасности при работе с вычислительной техникой; производить подключение блоков персонального компьютера и периферийных устройств; производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; выполнять инсталляцию системного и прикладного программного обеспечения; создавать и управлять содержимым документов с помощью текстовых процессоров; создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; создавать и управлять содержимым презентаций с помощью редакторов презентаций; использовать мультимедиа проектор для демонстрации презентаций; вводить, редактировать и удалять записи в базе данных; эффективно пользоваться запросами базы данных; создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; производить сканирование документов и их распознавание; производить распечатку, копирование и тиражирование документов на принтере и других устройствах; управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; осуществлять антивирусную защиту персонального компьютера с помощью антивирус-

	ных программ; осуществлять резервное копирование и восстановление данных
Приобрести первоначальный практический опыт	выполнения требований техники безопасности при работе с вычислительной техникой; организации рабочего места оператора электронно-вычислительных и вычислительных машин; подготовки оборудования компьютерной системы к работе; инсталляции, настройки и обслуживания программного обеспечения компьютерной системы; управления файлами; применения офисного программного обеспечения в соответствии с прикладной задачей; использования ресурсов локальной вычислительной сети; использования ресурсов, технологий и сервисов Интернет; применения средств защиты информации в компьютерной системе. *выбора рациональной конфигурации оборудования в соответствии с решаемой задачей* *создания форм и их защиты.* *работы с расширенной фильтрацией и условным форматированием* *применения триггеров при создании презентации* *создания связей таблиц по типу многие-ко-многим* *создания пиктограммы в графическом редакторе* *организации работ по использованию и применению политики безопасности организации* *персонализации работы антивирусных программ* *организации мероприятий по резервному восстановлению данных* *использования сервисов сети Интернет в профессиональной деятельности* *применения программных средств для мониторинга трафика*

1.3. Количество часов на освоение учебной практики:

Всего - 504 часа, в том числе в форме практической подготовки – 504 часа:

В рамках освоения ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении- 108 часов, в том числе в форме практической подготовки – 108 часов

В рамках освоения ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами - 144 часа, в том числе в форме практической подготовки – 144 часа

В рамках освоения ПМ.03 Защита информации техническими средствами- 144 часов, в том числе в форме практической подготовки – 144 часа

В рамках освоения ПМ.04 Выполнение работ по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин - 108 часов, в том числе в форме практической подготовки – 108 часов

II. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

2.1 Результатом освоения программы учебной практики является сформированность у обучающихся умений, приобретение первоначального практического опыта в рамках модулей ППССЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем по видам профессиональной деятельности (ВПД): эксплуатация автоматизированных (информационных) систем в защищенном исполнении, защита информации в автоматизированных системах программными и программно-аппаратными средствами, защита информации техническими средствами, выполнение работ по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин, необходимых для последующего освоения ими профессиональных (ПК) и общих (ОК) компетенций по избранной специальности и личностными результатами (ЛР).

2.2 Перечень профессиональных компетенций

Код	Наименование результата обучения
ВД.1	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
ВД.2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
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.
ВД.3	Защита информации техническими средствами

ПК 3.1	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5	Организовывать отдельные работы по физической защите объектов информатизации.
ВД.4	Выполнение работ по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин
ПК 4.1.	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК 4.4.	Обеспечивать применение средств защиты информации в компьютерной системе

2.3 Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.
ОК 11.	Планировать предпринимательскую деятельность в профессиональной сфере

2.4 Перечень личностных результатов

Код	Наименование результата обучения
ЛР 1.	Осознающий себя гражданином и защитником великой страны
ЛР 2.	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций
ЛР 3.	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
ЛР 4.	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР 5.	Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России
ЛР.6	Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях
ЛР.7	Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР.8	Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства
ЛР.9.	Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях
ЛР 10.	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой
ЛР 11.	Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры
ЛР 12.	Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания
ЛР КК 1.	Признающий ценность непрерывного образования, ориентирующийся в изменяющемся рынке труда, избегающий безработицы, управляющий собственным профессиональным развитием, рефлексивно оценивающий собственный жизненный опыт, критерии успешности
ЛР КК 2.	Экономически активный, предприимчивый, готовый к самозанятости

III. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

3.1. Тематический план учебной практики

Код ПК	Код и наименование профессионального модуля	Количество часов по ПМ	Виды работ	Наименование тем учебной практики	Количество часов
1	2	3	4	5	6
ПК 1.1 - 1.4	ПМ.01 Эксплуатация автоматизированных «Информационных» систем в защищенном исполнении	108	Проведение аудита защищенности автоматизированной системы	**Тема 1.1** Аудит защищенности автоматизированной системы	6
			Установка, настройка и эксплуатация сетевых операционных систем	**Тема 1.2** Установка и настройка сетевой ОС семейства Windows	6
				Тема 1.3 Установка и настройка сетевой ОС семейства Linux	6
			Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы	**Тема 1.4** Эксплуатация подсистем безопасности сетевых операционных систем	6
			Организация работ с удаленными хранилищами данных и базами данных	**Тема 1.5** Организация удаленной работы с хранилищами данных	6
			Организация защищенной передачи данных в компьютерных сетях	**Тема 1.6** Защищенная передача данных в компьютерных сетях	6
			Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов	**Тема 1.7** Конфигурирование локальных сетей	6
				Тема 1.8 Монтаж ЛВС	6
				Тема 1.9 Установление и настройка параметров современных сетевых протоколов	6
			Осуществление диагностики компьютерных сетей, определе-	**Тема 1.10** Диагностика компьютерных сетей	6

			ние неисправностей и сбоев подсистемы безопасности и устранение неисправностей	Тема 1.11 Устранение неисправностей в работе ЛВС	6
			Настройка программно-аппаратных средств защиты информации, в тома числе антивирусной защиты в операционных системах по заданным шаблонам	Тема 1.12 Настройка и оптимизация работы программно-аппаратных средств защиты информации	6
			Инструктаж пользователей по порядку работы в операционных системах	Тема 1.13 Инструктаж по работе с ОС	6
			Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах	Тема 1.14 Эксплуатационная документация на программно-аппаратные средства защиты информации в операционных системах	6
			Ввод в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях	Тема 1.15 Программно-аппаратные средства защиты информации в компьютерных сетях	6
				Тема 1.16 Установка межсетевого экрана	6
				Тема 1.17 Оптимизация работы межсетевого экрана на примере ASA	6
			Дифференцированный зачет		6
Всего часов					108

Код ПК	Код и наименование профессионального модуля	Количество часов по ПМ	Виды работ	Наименование тем учебной практики	Количество часов
1	2	3	4	5	6
ПК 2.1 - 2.6	**ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами**	144	Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах	**Тема 2.1** Программные средства обеспечения информационной безопасности в автоматизированных системах	6
				Тема 2.2 Программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах	6
			Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности	**Тема 2.3** Диагностика и устранение отказов программно-аппаратных средств обеспечения информационной безопасности	6
				Тема 2.4 Обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности	6
			Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности	**Тема 2.5** Эффективность использования программно-аппаратных средств обеспечения информационной безопасности	6
			Составление документации по учету, обработке, хранению и передаче конфиденциальной информации	**Тема 2.6** Организация ведения конфиденциального документооборота	12
			Использование программного обеспечения для обработки, хранения и	**Тема 2.7** Программное обеспечение для обработки, хранения и	12

			передачи конфиденциальной информации	передачи конфиденциальной информации	
			Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов	Тема 2.8 Проведение различных видов контрольных проверок при аттестации объектов	12
			Устранение замечаний по результатам проверки	Тема 2.9 Устранение замечаний по результатам аудита	12
			Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов	Тема 2.10 Нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами	12
			Применение математических методов для оценки качества и выбора наилучшего программного средства	Тема 2.11 Оценка качества программных продуктов	6
			Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи	Тема 2.12 Криптографические средства и методы защиты информации	12
			Определение правил и процедур управления системой защиты информации автоматизированной системы	Тема 2.13 Управление системой защиты информации автоматизированной системы	6
			Определение правил и процедур выявления инцидента	Тема 2.14 Выявление инцидентов	6
			Определение правил и процедур реагирования на инциденты	Тема 2.15 Процедуры реагирования на инциденты	6

			Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации	**Тема 2.15** Вывод автоматизированной системы из эксплуатации	12
			Дифференцированный зачет		6
Всего часов					144

Код ПК	Код и наимснование профессиональн ого модуля	Колич ество часов по ПМ	Виды работ	Наименование тем учебной практики	Колич ество часов
1	2	3	4	5	6
ПК 3.1 - 3.5	**ПМ.03 Защита информации техническими средствами**	144	Измерение параметров физических полей	Тема 3.1 Параметры физических полей	6
			Определение каналов утечки ПЭМИН.	Тема 3.2 Каналы утечки ПЭМИН.	6
			Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	Тема 3.3 Измерение параметров фоновых шумов и физических полей	6
			Установка и настройка технических средств защиты информации.	Тема 3.4 Технические средства защиты информации	12
			Проведение измерений параметров побочных электромагнитных излучений и наводок.	Тема 3.5 Параметры побочных электромагнитных излучений и наводок	6
			Проведение аттестации объектов информатизации.	Тема 3.6 Аттестация объектов информатизации	12
			Монтаж различных типов датчиков.	Тема 3.7 Монтаж датчиков	6
			Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.	Тема 3.8 Системы пожарно-охранной сигнализации	6
			Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.	Тема 3.9 Промышленное оборудование для защиты информации	6
			Рассмотрение системы контроля и управления доступом.	Тема 3.10 Системы контроля и управления доступом.	12
			Рассмотрение принци-	Тема 3.11	6

			пов работы системы видеонаблюдения и ее проектирование.	Принципы работы системы видеонаблюдения	
			Рассмотрение датчиков периметра, их принципов работы.	**Тема 3.12** Принципы работы датчиков периметра	6
			Выполнение звукоизоляции помещений системы зашумления.	**Тема 3.13** Система зашумления	6
			Реализация защиты от утечки по цепям электропитания и заземления.	**Тема 3.14** Защита от утечки по цепям электропитания и заземления	6
			Разработка организационных и технических мероприятий по заданию преподавателя;	**Тема 3.15** Организационные и технические мероприятия по защите информации	12
			Разработка основной документации по инженерно-технической защите информации.	**Тема 3.16** Документация по инженерно-технической защите информации.	6
			Корректировка конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки, контроля и испытаний.	**Тема 3.17** Конструкторская документация на изготовление средства защиты информации от несанкционированного доступа	6
			Отработка конструкции средства защиты информации на технологичность с учетом стандартов ЕСТД;	**Тема 3.18** Конструкция средства защиты информации от несанкционированного доступа	6
			Заключение договоров с поставщиками комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности	**Тема 3.19** Документация по приобретению комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной	6

			собственности	
			Промежуточная аттестация в форме дифференцированного зачета	6
	Всего часов			144

Код ПК	Код и наименование профессионального модуля	Количество часов по ПМ	Виды работ	Наименование тем учебной практики	Количество часов
1	2	3	4	5	6
ПК 4.1.-4.4.	ПМ.04 Выполнение работ по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин	108	Соблюдение техники безопасности при работе на ЭВМ Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка Установка и замена расходных материалов для принтеров, ксерокса, плоттера. *Выбор рациональной конфигурации оборудования в соответствии с решаемой задачей*	Тема 1.1. Работа с устройствами компьютерной системы	8
			Установка операционной среды, настройка интерфейса ОС (рабочий стол, безопасность системы, подключение к сети). Установка прикладных программ. Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете	Тема 1.2. Работа с программным обеспечением компьютерной системы	6
			Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей экс-	Тема 1.3. Диагностика неисправностей системы, ведение документации	6

			плуатации ЭВМ		
			Сканирование текстовых документов и их распознавание Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации, сохранение докумснтов Форматирование и редактирование документов в текстовом процессоре. Работа с таблицами в текстовом процессоре. Работа с диаграммами в текстовом процессоре. Работа с графическими объектами в текстовом процессоре. Печать документов в текстовом процессоре.	Тема 2.1. Работа в текстовом процессоре	16
			Создание и форматирование таблицы в редакторе электронных таблиц Вычисление с помощью формул в электронной таблице Работа со встроснными функциями в электронной таблице Работа со списками в электронной таблице Создание форм для ввода данных в таблицы Создание и работа с диаграммами и графиками Обмен данными между текстовым процессором и электронной таблицей *Работа с расширенной*	Тема 2.2. Работа в редакторе электронных таблиц	16

			фильтрацией и условным форматированием		
			Построение презентации различными способами. Обработка объектов слайдов презентации. Настройка анимации объектов. Настройка показа и демонстрация результатов работы средствами мультимедиа. *Применение триггеров при создании презентации.*	Тема 2.3. Работа в программе подготовки и просмотра презентаций	8
			Ввод данных в таблицы базы данных. Создание простых запросов без параметров и с параметрами. Создание отчетов. *Создание форм и их защита.* *Создание связей таблиц по типу многие-ко-многим.*	Тема 2.4. Работа в системе управления базами данных	8
			Рисование объектов средствами графического редактора. Работа с заливками и контурами в программе векторной графики. Работа с текстом в программе векторной графики. Работа с эффектами программе векторной графики. Вставка и редактирование готового изображения с использованием программ растровой графики. Работа с цветом с использованием про-	Тема 2.5. Работа в графических редакторах	8

			грамм растрой графики. Работа со слоями с использованием программ растрой графики. Работа со спецэффектами с использованием программ растровой графики. *Создание пиктограммы в графическом редакторе.*		
			Создание и обмен письмами электронной почты. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера. Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов. Пересылка и публикация файлов данных в Интернете.	Тема 3.1. Работа с ресурсами Интернета	8
			Использование штатных средств защиты операционной системы и прикладных программ. Применение парольной защиты. Установка антивирусных программ, их настройка. Обновление базы. Выполнение архивирования данных. Выполнение резервного копирования и восстановления данных	Тема 4.1. Защита информации при работе с офисными приложениями	10
			Организация работ по использованию и при-	*Тема 5.1. Персонализация мероприятий ин-*	8

			менению политики безопасности организации *Персонализация работы антивирусных программ.* *Организация мероприятий по резервному восстановлению данных* *Использование сервисов сети Интернет в профессиональной деятельности.* *Применение программных средств для мониторинга трафика.*	*формационной безопасности*	
			Промежуточная аттестация в форме дифференцированного зачета		6
	Всего часов				108

3.2. Содержание учебной практики

Содержание учебной практики определяется требованиями к умениям и практическому опыту в рамках модуля ОПОП СПО по видам профессиональной деятельности (ВПД): эксплуатация автоматизированных (информационных) систем в защищенном исполнении, защита информации в автоматизированных системах программными и программно-аппаратными средствами, защита информации техническими средствами, выполнение работ по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин.

Код и наименование профессиональных модулей и тем учебной практики	**Содержание учебных занятий**	Объем часов	Уровень усвоения
ПМ.01 Планирование и организация работ по обеспечению защиты объекта		108	
Проведение аудита защищенности автоматизированной системы Установка, настройка и эксплуатация сетевых операционных систем Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы Организация работ с удаленными хранилищами данных и базами данных Организация защищенной передачи данных в компьютерных сетях Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов Осуществление диагностики компьютер-			

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
ных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей *Настройка программно-аппаратных средств защиты информации, в тома числе антивирусной защиты в операционных системах по заданным шаблонам* *Инструктаж пользователей по порядку работы в операционных системах* *Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах* *Ввод в эксплуатацию программно-аппаратных средств за щиты информации в компьютерных сетях*			
Тема 1.1. Аудит защищенности автоматизированной системы	**Содержание:**	6	2
	1. Практическое занятие №1. Ознакомление с правилами техники безопасности при работе с ПК, оргтехникой.	2	
	2. Практическое занятие №2. Обзор компонентов защищенной информационной системы	2	
	3. Практическое занятие №3. Проведение аудита информационной системы	2	
Тема 1.2 Установка и настройка сетевой ОС семейства Windows	**Содержание:**	6	2
	1. Практическое занятие №4. Создание дистрибутива	2	
	2. Практическое занятие №5. Установка Windows Server 2016 на виртуальную машину	2	
	3. Практическое занятие №6.	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	Настройка политик безопасности Windows Server 2016		
Тема 1.3. Установка и настройка сетевой ОС семейства Linux	**Содержание:**	6	2
	1. Практическое занятие № 7. Создание дистрибутива	2	
	2. Практическое занятие № 8. Установка Centos 7.0 на виртуальную машину	2	
	3. Практическое занятие № 9. Настройка политик безопасности Centos 7.0	2	
Тема 1.4. Эксплуатация подсистем безопасности сетевых операционных систем	**Содержание:**	6	2
	1. Практическое занятие № 10. Национальные стандарты в области защиты информации.	2	
	2. Практическое занятие № 11. Настройка политик безопасности в сетевой операционной системе	2	
	3. Практическое занятие № 12. Контроль работоспособности подсистем безопасности сетевых операционных систем	2	
Тема 1.5. Организация удаленной работы с хранилищами данных	**Содержание:**	6	2
	1. Практическое занятие № 13. Помещение и передача файлов в хранилище данных.	2	
	2. Практическое занятие № 14. Организация хранения файлов в хранилищах данных.	2	
	3. Практическое занятие № 15. Документирование работы с хранилищами данных.	2	
Тема 1.6. Защищенная передача данных в компьютерных сетях	**Содержание:**	6	2
	1. Практическое занятие № 16. Ограничение доступа в помещения, в которых происходит подготовка и обработка информации	2	
	2. Практическое занятие № 17. Хранение электронных носителей и регистрационных журналов в закрытых для доступа посторонних лиц помещениях	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	3. Практическое занятие № 18. Организация контроля трафика в сетевом пространстве	2	
Тема 1.7. Конфигурирование локальных сетей	Содержание:	6	2
	1. Практическое занятие № 19. Определение топологии ЛВС согласно специфике деятельности организации	2	
	2. Практическое занятие № 20. Определение компонентов сетевой инфраструктуры.	2	
	3. Практическое занятие № 21. Проектирование сетевой инфраструктуры организации.	2	
Тема 1.8. Монтаж ЛВС	Содержание:	6	2
	1. Практическое занятие № 22. Монтаж патч-кордов по стандарту TIA-A (B).	2	
	2. Практическое занятие № 23. Монтаж кабель-каналов.	2	
	3. Практическое занятие № 24. Монтаж распределительной панели.	2	
Тема 1.9. Установление и настройка параметров современных сетевых протоколов	Содержание:	6	2
	1. Практическое занятие № 25. Установка и настройка протокола TCP/IP.	2	
	2. Практическое занятие № 26. Настройка дополнительных параметров протокола TCP/IP.	2	
	3. Практическое занятие № 27. Диагностика и устранение неполадок TCP/IP	2	
Тема 1.10. Диагностика компьютерных сетей	Содержание:	6	2
	1. Практическое занятие № 28. Диагностика и устранение ошибок в работе штатными средствами Windows	2	
	2. Практическое занятие № 29. Тестирование трассировкой	2	
	3. Практическое занятие № 30. Тестирование отдельных протоколов	2	
Тема 1.11.	Содержание:	6	2

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
Устранение неисправностей в работе ЛВС	**1. Практическое занятие № 31.** Организация диагностики работоспособности ЛВС	2	
	2. Практическое занятие № 32. Устранение возникших неисправностей штатными средствами.	2	
	3. Практическое занятие № 33. Документирование проблемы и ее решения.	2	
Тема 1.12. Настройка и оптимизация работы программно-аппаратных средств защиты информации	**Содержание:**	6	2
	1. Практическое занятие № 34. Средства архивации информации	2	
	2. Практическое занятие № 35. Антивирусные программы	2	
	3. Практическое занятие № 36. Идентификация и аутентификация пользователя	2	
Тема 1.13. Инструктаж по работе с ОС.	**Содержание:**	6	2
	1. Практическое занятие № 37. Основные требования к безопасной эксплуатации операционной системы.	2	
	2. Практическое занятие № 38. Основные факторы, влияющие на работоспособность информационной системы.	2	
	3. Практическое занятие № 39. Планирование функционирования и оптимизация работы ОС	2	
Тема 1.14. Эксплуатационная документация на программно-аппаратные средства защиты информации в операционных системах	**Содержание:**	6	2
	1. Практическое занятие № 40. Эксплуатационная документация на средства архивации данных	2	
	2. Практическое занятие № 41. Эксплуатационная документация на средства идентификации пользователей	2	
	3. Практическое занятие № 42. Эксплуатационная документация на средства и аутентификации пользователей.	2	
Тема 1.15. Программно-аппаратные средства за щиты информации в компьютер-	**Содержание:**	6	2
	1. Практическое занятие № 43. Показатели эффективности систем защиты	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
ных сетях	информации		
	2. Практическое занятие № 44. Методы и средства защиты информации в операционной системе UNIX	2	
	3. Практическое занятие № 45. Методы и средства защиты информации в операционной системе Windows.	2	
Тема 1.16. Установка межсетевого экрана	**Содержание:**	**6**	2
	1. **Практическое занятие № 46.** Установка межсетевого экрана Comodo	2	
	2. **Практическое занятие № 47.** Параметры администрирования межсетевого экрана Comodo	2	
	3. **Практическое занятие № 48.** Установка межсетевого экрана ASA	2	
Тема 1.17. Оптимизация работы межсетевого экрана на примере ASA	**Содержание:**	**6**	2
	1. **Практическое занятие № 49.** Подключение ресурсов локальной сети к сети Интернет с использованием динамической трансляции адресов (SNAT)	2	
	2. **Практическое занятие № 50.** Контентная фильтрация ASA	2	
	3. **Практическое занятие № 51.** Экспорт событий системных журналов на выделенные сервера (Syslog).	2	
Промежуточная аттестация в форме дифференцированного зачета		**6**	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		**144**	
Применение программных и			

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности Составление документации по учету, обработке, хранению и передаче конфиденциальной информации Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов Устранение замечаний по результатам проверки Анализ и составление			

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов Применение математических методов для оценки качества и выбора наилучшего программного средства Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи *Определение правил и процедур управления системой защиты информации автоматизированной системы* *Определение правил и процедур выявления инцидента* *Определение правил и процедур реагирования на инциденты* *Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации*			
Тема 2.1. Программные средства обеспечения информационной безопасности в ав-	**Содержание:**	6	2
	1. Практическое занятие № 1. Организация и разграничение доступа к данным и ресурсам системы	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
томатизированных системах	**2. Практическое занятие № 2.** Контроль всех операций изменения информации и защита данных при их обработке	2	
	3. Практическое занятие № 3. Контроль и защита данных при их передаче в сети автоматизированной системы.	2	
Тема 2.2. Программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах	**Содержание:**	6	2
	1. Практическое занятие № 4. Дублирование (резервирование) информации	2	
	2. Практическое занятие № 5. Блокировка ошибочных операций	2	
	3. Практическое занятие № 6. Защита от вредительских программ	2	
Тема 2.3. Диагностика и устранение отказов программно-аппаратных средств обеспечения информационной безопасности	**Содержание:**	6	2
	1. Практическое занятие № 7. Регистрация событий и аудит	2	
	2. Практическое занятие № 8. Проведение диагностики в работе межсетевых экранов	2	
	3. Практическое занятие № 9. Устранение отказов в работе программно-аппаратных средств обеспечения информационной безопасности	2	
Тема 2.4. Обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности	**Содержание:**	6	2
	1. Практическое занятие № 10. Обеспечение работоспособности средств обеспечивающих защиту от внешних событий	2	
	2. Практическое занятие № 11. Обеспечение работоспособности средств обеспечивающих защиту от внутренних событий	2	
	3. Практическое занятие № 12. Обнаружение атак программными средствами	2	
Тема 2.5. Эффективность использования программно-аппаратных средств обеспечения информационной безопасности	**Содержание:**	6	2
	1. Практическое занятие № 13. Эффективность применения файрвола SOHO	2	
	2. Практическое занятие № 14. Эффективность применения файрвола Cisco ASA	2	
	3. Практическое занятие № 15. Настройка файрвола встроенными средствами Linux	2	
Тема 2.6. Организация ведения конфиденци-	**Содержание:**	12	2
	1. Практическое занятие № 16.	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
ального документо-оборота	Разрешительная система доступа к конфиденциальным документам		
	2. Практическое занятие № 17. Исключение несанкционированного доступа к конфиденциальным документам	2	
	3. Практическое занятие № 18. Целенаправленное регулирование процессов движения конфиденциальных документов	2	
	4. Практическое занятие № 19. Фиксированная передача конфиденциальных документов	2	
	5. Практическое занятие № 20. Обеспечение своевременного и качественного исполнения конфиденциальных документов	2	
	6. Практическое занятие № 21. Персональная и обязательная ответственность за выдачу неправомерных разрешений на ознакомление с конфиденциальными документами и на их отправление	2	
Тема 2.7. Программное обеспечение для обработки, хранения и передачи конфиденциальной информации	Содержание:	12	2
	1. Практическое занятие № 22. Применение офисных пакстов для ведения документооборота, содержащего конфиденциальную информацию	2	
	2. Практическое занятие № 23. Оценка эффективности использования стандартного программного обеспечения для ведения конфиденциального документооборота	2	
	3. Практическое занятие № 24. Применение пакетов прикладных программ для ведения электронного конфиденциального документооборота	2	
	4. Практическое занятие № 25. Эффективность использования системы DIRECTUM 4.9 как элемента системы средств криптографической защиты информации (СКЗИ)	2	
	5. Практическое занятие № 26. Возможности системы «Приоритет»	2	
	6. Практическое занятие № 27. Возможности модуля "Синхронизация файлов	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	1С:Документооборот с облачным хранилищем"		
Тема 2.8. Проведение различных видов контрольных проверок при аттестации объектов	**Содержание:**	12	2
	1. Практическое занятие № 28. Анализ исходных данных по аттестуемому объекту информатизации	2	
	2. Практическое занятие № 29. Предварительное ознакомление с аттестуемым объектом информатизации	2	
	3. Практическое занятие № 30. Первичный осмотр помещений	2	
	4. Практическое занятие № 31. Проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств	2	
	5. Практическое занятие № 32. Проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации	2	
	6. Практическое занятие № 33. Проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации	2	
Тема 2.9. Устранение замечаний по результатам аудита	**Содержание:**	12	2
	1. Практическое занятие № 34. Подготовка пояснительной записки, содержащей информационную характеристику и организационную структуру объекта защиты	2	
	2. Практическое занятие № 35. Корректировка перечня объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты	2	
	3. Практическое занятие № 36. Корректировка перечня выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории за-	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	щиты		
	4. Практическое занятие № 37. Корректировка схемы систем активной защиты	2	
	5. Практическое занятие № 38. Подготовка апелляции	2	
	6. Практическое занятие № 39. Подготовка пакета документов для передачи в орган аттестации	2	
Тема 2.10. Нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами	Содержание:	12	2
	1. Практическое занятие № 40. Организационные документы, устанавливающие принципы, требования и способы противодействия пассивным угрозам ценной информации	2	
	2. Практическое занятие № 41. Организационные документы, устанавливающие принципы, требования и способы противодействия активным угрозам ценной информации	2	
	3. Практическое занятие № 42. Инструктивные документы, устанавливающие принципы, требования и способы противодействия пассивным угрозам ценной информации	2	
	4. Практическое занятие № 43. Инструктивные документы, устанавливающие принципы, требования и способы противодействия активным угрозам ценной информации	2	
	5. Практическое занятие № 44. Информационные документы, устанавливающие принципы, требования и способы противодействия пассивным угрозам ценной информации	2	
	6. Практическое занятие № 45. Информационные документы, устанавливающие принципы, требования и способы противодействия активным угрозам ценной информации	2	
Тема 2.11. Оценка качества программных продуктов	Содержание:	6	2
	1. Практическое занятие № 46. Качество программного обеспечения	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	2. Практическое занятие № 47. Качество программного средства	2	
	3. Практическое занятие № 48. Оценка качества по стандарту ISO 9126	2	
Тема 2.12. Криптографические средства и методы защиты информации	**Содержание:**	12	2
	1. Практическое занятие № 49. Минимизация вероятности преодоления («взлома») защиты	2	
	2. Практическое занятие № 50. Создание надежного, недоступного для других канала связи между абонентами	2	
	3. Практическое занятие № 51. Применение симметричных алгоритмов шифрования	2	
	4. Практическое занятие № 52. Применение асимметричных алгоритмов шифрования	2	
	5. Практическое занятие № 53. Алгоритм RSA	2	
	6. Практическое занятие № 54. Электронная подпись	2	
Тема 2.13. Управление системой защиты информации автоматизированной системы	**Содержание:**	6	2
	1. Практическое занятие № 55. Организация политик безопасности, направленных на определение действий внутреннего злоумышленника	2	
	2. Практическое занятие № 56. Управление системой защиты информации от копирования на съемные носители	2	
	3. Практическое занятие № 57. Эксплуатация уязвимостей системного и прикладного ПО и аппаратных устройств	2	
Тема 2.14. Выявление инцидентов	**Содержание:**	6	2
	1. Практическое занятие № 58. Ликвидация последствий внедрения вредоносного ПО в систему управления	2	
	2. Практическое занятие № 59. Определение несанкционированного доступа к каналам передачи данных	2	
	3. Практическое занятие № 60. Определение атак, влекущих ущерб информа-	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	ционной системе		
Тема 2.15. Процедуры реагирования на инциденты	**Содержание:**	**6**	2
	1. Практическое занятие № 61. Устранение закладок в ПО и аппратных средствах	**2**	
	2. Практическое занятие № 62. Ликвидация последствий внедрения вредоносного ПО в систему управления	**2**	
	3. Практическое занятие № 63. Ликвидация последствий от физического подключения к каналам передачи данных	**2**	
Тема 2.16 Вывод автоматизированной системы из эксплуатации	**Содержание:**	**12**	2
	1. Практическое занятие № 64. Определение нецелесообразности эксплуатации системы	**2**	
	2. Практическое занятие № 65. Расчет финансово-экономической неэффективности эксплуатации системы	**2**	
	3. Практическое занятие № 66. Подготовка оснований для вывода системы из эксплуатации	**2**	
	4. Практическое занятие № 67. Разработка перечня и сроков реализации мероприятий по выводу системы из эксплуатации	**2**	
	5. Практическое занятие № 68. Подготовка правового акта о выводе системы из эксплуатации	**2**	
	6. Практическое занятие № 69. Соблюдение требований постановления Правительства РФ от 6 июля 2015 г. N 676	**2**	
Промежуточная аттестация в форме дифференцированного зачета		6	
ПМ.03 Защита информации техническими средствами		**144**	
Измерение параметров физических полей Определение каналов утечки ПЭМИН. Проведение измерений			

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Установка и настройка технических средств защиты информации. Проведение измерений параметров побочных электромагнитных излучений и наводок. Проведение аттестации объектов информатизации. Монтаж различных типов датчиков. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. Рассмотрение системы контроля и управления доступом. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы. Выполнение звукоизоляции помещений си-			

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
стемы зашумления. Реализация защиты от утечки по цепям электропитания и заземления. Разработка организационных и технических мероприятий по заданию преподавателя; Разработка основной документации по инженерно-технической защите информации. *Корректировка конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки, контроля и испытаний.* *Отработка конструкции средства защиты информации на технологичность с учетом стандартов ЕСТД;* *Заключение договоров с поставщиками комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности*			
Тема 3.1 Параметры физических полей	**Содержание:**	6	
	1. Практическое занятие № 1 Измерение напряженности электромагнитного	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	поля		
	2. Практическое занятие № 2 Оптические измерения	2	
	3. Практическое занятие № 3 Акустические измерения	2	
Тема 3.2 Каналы утечки ПЭМИН	**Содержание:**	6	
	1. Практическое занятие № 4 Определение побочных электромагнитных излучений и наводок	2	
	2. Практическое занятие № 5 Восстановление информации при перехвате ПЭМИН	2	
	3. Практическое занятие № 6 Восстановление информации при перехвате ПЭМИН	2	
Тема 3.3 Измерение параметров фоновых шумов и физических полей	**Содержание:**	6	
	1. Практическое занятие № 7 Средства измерения параметров физических факторов	2	
	2. Практическое занятие № 8 Измерение корректированного виброускорения, виброскорости, виброперемещения	2	
	3. Практическое занятие № 9 Измерение общей и локальной вибрации, воздействующей на человека	2	
Тема 3.4 Технические средства защиты информации	**Содержание:**	12	
	1. Практическое занятие № 10 Средства обнаружения	2	
	2. Практическое занятие № 11 Средства поиска и детальных измерений	2	
	3. Практическое занятие № 12 Средства активного и пассивного противодействия	2	
	4. Практическое занятие № 13 Проведение специальных исследований технических средств на наличие возможных каналов утечки информации	2	
	5. Практическое занятие № 14 Локализация каналов утечки информации	2	
	6. Практическое занятие № 15 Противодействие несанкционированному доступу к источникам конфиденциальной ин-	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	формации		
Тема 3.5 Параметры побочных электромагнитных излучений и наводок	**Содержание:**	6	
	1. Практическое занятие № 16 Низкочастотные излучения технических средств	2	
	2. Практическое занятие № 17 Высокочастотные излучения технических средств	2	
	3. Практическое занятие № 18 Протоколирование измерений	2	
Тема 3.6 Аттестация объектов информатизации	Содержание:	12	
	1. Практическое занятие № 19 Подготовка документации в орган аттестации	2	
	2. Практическое занятие № 20 Подготовка к первичному осмотру помещений	2	
	3. Практическое занятие № 21 Проведение первичного осмотра помещений	2	
	4. Практическое занятие № 22 Проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации	2	
	5. Практическое занятие № 23 Проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации	2	
	6. Практическое занятие № 24 Подготовка комплекта документов в орган аттестации	2	
Тема 3.7 Монтаж датчиков	Содержание:	6	
	1. Практическое занятие № 25 Монтаж датчиков пожарной сигнализации	2	
	2. Практическое занятие № 26 Монтаж датчиков движения	2	
	3. Практическое занятие №Монтаж 27 Монтаж датчиков температуры	2	
Тема 3.8 Системы пожарно-охранной сигнализации	Содержание:	6	
	1. Практическое занятие № 28 Прокладка кабелей путем штробления	2	
	2. Практическое занятие № 29	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	Прокладка кабелей при помощи кабель-канала и гофрированной трубы		
	3. Практическое занятие № 30 Монтаж пожарных извещателей, оповещателей и приемно-контрольных приборов	2	
Тема 3.9 Промышленное оборудование для защиты информации	**Содержание:**	6	
	1. Практическое занятие № 31 Подавители связи	2	
	2. Практическое занятие № 32 Блокираторы Сотовой связи и беспроводного доступа	2	
	3. Практическое занятие № 33 Генераторы для защиты информации от утечки по каналам побочных электромагнитных излучений и наводок на линии электропитания и заземления	2	
Тема 3.10 Системы контроля и управления доступом.	**Содержание:**	12	
	1. Практическое занятие № 34 Монтаж преграждающих устройств	2	
	2. Практическое занятие № 35 Эффективность использования преграждающих устройств	2	
	3. Практическое занятие № 36 Идентификаторы	2	
	4. Практическое занятие № 37 Монтаж вспомогательного оборудования	2	
	5. Практическое занятие № 38 Монтаж исполнительных устройств	2	
	6. Практическое занятие № 39 Автономные системы управления доступом	2	
Тема 3.11 Принципы работы системы видеонаблюдения	**Содержание:**	6	
	1. Практическое занятие № 40 Проектирование плана установки камер видеонаблюдения с учетом требований нормативной документации	2	
	2. Практическое занятие № 41 Монтаж аналоговых систем видеонаблюдения	2	
	3. Практическое занятие № 42 Монтаж цифровых систем видеонаблюдения	2	
Тема 3.12 Принципы работы датчиков пе-	**Содержание:**	6	
	1. Практическое занятие № 43	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
риметра	Принцип работы инфракрасных детекторов		
	2. Практическое занятие № 44 Принцип работы ультразвуковых детекторов	**2**	
	3. Практическое занятие № 45 Принцип работы лазерных приборов	**2**	
Тема 3.13 Система зашумления	**Содержание:**	**6**	
	1. Практическое занятие № 46 Системы линейного зашумления	**2**	
	2. Практическое занятие № 47 Системы пространственного зашумления	**2**	
	3. Практическое занятие № 48 Метод "синфазной" маскирующей низкочастотной помехи	**2**	
Тема 3.14 Защита от утечки по цепям электропитания и заземления	**Содержание:**	**6**	
	1. Практическое занятие № 49 Предотвращение переизлучения электромагнитного излучения	**2**	
	2. Практическое занятие № 50 Эквивалентная схема нежелательной асимметричной связи двух устройств	**2**	
	3. Практическое занятие № 51 Комплекс мер, направленных на защиту от утечки по цепям электропитания и заземления	**2**	
Тема 3.15 Организационные и технические мероприятия по защите информации	**Содержание:**	**12**	
	1. Практическое занятие № 52 Государственное регулирование в области защиты информации	**2**	
	2. Практическое занятие № 53 Лицензирование деятельности юридических и физических лиц в области защиты информации	**2**	
	3. Практическое занятие № 54 Сертификация и аттестация средств защиты информации	**2**	
	4. Практическое занятие № 55 Организационно-административные методы защиты информации	**2**	
	5. Практическое занятие № 565 Организационно-технические методы защиты информации	**2**	
	6. Практическое занятие № 57	**2**	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	Страхование как метод защиты информации		
Тема 3.16 Документация по инженерно-технической защите информации	**Содержание:**	6	
	1. Практическое занятие № 58 Руководящие документы организации инженерно-технической защиты информации	2	
	2. Практическое занятие № 59 Нормативные документы организации инженерно-технической защиты информации	2	
	3. Практическое занятие № 60 Методические документы организации инженерно-технической защиты информации	2	
Тема 3.17 Конструкторская документация на изготовление средства защиты информации от несанкционированного доступа	**Содержание:**	6	
	1. Практическое занятие № 61 Внесение изменений в документацию межсетевых экранов	2	
	2. Практическое занятие № 62 Корректировка документации средств вычислительной техники по защите от несанкционированного доступа к информации	2	
	3. Практическое занятие № 63 Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации	2	
Тема 3.18 Конструкция средства защиты информации от несанкционированного доступа	**Содержание:**	6	
	1. Практическое занятие № 64 Определение задач, решаемых средствами защиты информации от несанкционированного доступа	2	
	2. Практическое занятие № 65 ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»	2	
	3. Практическое занятие № 66 Требования руководящих документов ФСТЭК России к средствам защиты информации от несанкционированного доступа	2	
Тема 3.19 Документация по приобретению	**Содержание:**	6	
	1. Практическое занятие № 67	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности	Заключение договоров с поставщиками комплектующих изделий и материалов		
	2. Практическое занятие № 68 Заключение лицензионных соглашений с правообладателями на использование объектов промышленной собственности	**2**	
	3. Практическое занятие № 69 Заключение лицензионных соглашений с правообладателями на использование объектов интеллектуальной собственности	**2**	
Промежуточная аттестация в форме дифференцированного зачета		6	
ПМ.04 Оператор электронно-вычислительных и вычислительных машин		**108**	
Виды работ: Соблюдение техники безопасности при работе на ЭВМ Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка Установка и замена расходных материалов для принтеров, ксерокса, плоттера. Выбор рациональной конфигурации оборудования в соответствии с решаемой задачей Установка операционной среды, настройка интерфейса ОС (рабочий стол, безопасность системы, подключение к сети). Установка прикладных программ. Управление файлами			

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ Сканирование текстовых документов и их распознавание Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации, сохранение документов Форматирование и редактирование документов в текстовом процессоре. Работа с таблицами в текстовом процессоре. Работа с диаграммами в текстовом процессоре. Работа с графическими объектами в текстовом процессоре. Печать документов в текстовом процессоре. Создание и форматирование таблицы в редакторе электронных таблиц Вычисление с помо-			

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
щью формул в электронной таблице Работа со встроенными функциями в электронной таблице Работа со списками в электронной таблице Создание форм для ввода данных в таблицы Создание и работа с диаграммами и графиками Обмен данными между текстовым процессором и электронной таблицей Работа с расширенной фильтрацией и условным форматированием Построение презентации различными способами. Обработка объектов слайдов презентации. Настройка анимации объектов. Настройка показа и демонстрация результатов работы средствами мультимедиа. Применение триггеров при создании презентации. Ввод данных в таблицы базы данных. Создание простых запросов без параметров и с параметрами. Создание отчетов. Создание форм и их защита. Создание связей таблиц по типу многие-ко-многим. Рисование объектов средствами графиче-			

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
ского редактора. Работа с заливками и контурами в программе векторной графики. Работа с текстом в программе векторной графики. Работа с эффектами программе векторной графики. Вставка и редактирование готового изображения с использованием программ растровой графики. Работа с цветом с использованием программ растрой графики. Работа со слоями с использованием программ растрой графики. Работа со спецэффектами с использованием программ растровой графики. Создание пиктограммы в графическом редакторе. Создание и обмен письмами электронной почты. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера. Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов. Пересылка и публикация файлов данных в Интернете. Использование штатных средств защиты операционной системы			

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
и прикладных программ. Применение парольной защиты. Установка антивирусных программ, их настройка. Обновление базы. Выполнение архивирования данных. Выполнение резервного копирования и восстановления данных Организация работ по использованию и применению политики безопасности организации Персонализация работы антивирусных программ. Организация мероприятий по резервному восстановлению данных Использование сервисов сети Интернет в профессиональной деятельности. Применение программных средств для мониторинга трафика.			
Раздел 1. Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения		**20**	
Тема 1.1. Работа с устройствами компьютерной системы	**Содержание:**	**8**	
	1. Практическое занятие №1. **Соблюдение техники безопасности при работе на ЭВМ. Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ**	2	
	2. Практическое занятие №2. **Работа с дополнительными внешними**	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	устройствами ПК: поиск драйверов, подключение, настройка		
	3. Практическое занятие №3. **Установка и замена расходных материалов для принтеров, ксерокса, плоттера.**	2	
	4. Практическое занятие №4. ***Выбор рациональной конфигурации оборудования в соответствии с решаемой задачей***	2	
Тема 1.2. Работа с программным обеспечением компьютерной системы	**Содержание:**	6	
	1. Практическое занятие №5. **Установка операционной среды, настройка интерфейса ОС** (рабочий стол, безопасность системы, подключение к сети).	2	
	2. Практическое занятие №6. **Установка прикладных программ.**	2	
	3. Практическое занятие №7. **Управление файлами данных** на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете.	2	
Тема 1.3. Диагностика неисправностей системы, ведение документации	**Содержание:**	6	
	1. Практическое занятие №8. **Диагностика простейших неисправностей персонального компьютера и периферийного оборудования**	2	
	2. Практическое занятие №9. **Диагностика простейших неисправностей компьютерной оргтехники**	2	
	3. Практическое занятие №10. **Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ**	2	
Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах		56	
Тема 2.1.	**Содержание:**	16	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
Работа в текстовом процессоре	**1. Практическое занятие №11. Сканирование текстовых документов и их распознавание**	2	
	2. Практическое занятие №12. Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации, сохранение документов.	2	
	3. Практическое занятие №13. Редактирование документов в текстовом процессоре.	2	
	4. Практическое занятие №14. Форматирование документов в текстовом процессоре..	2	
	5. Практическое занятие №15. Работа с таблицами в текстовом процессоре.	2	
	6. Практическое занятие №16. Работа с диаграммами в текстовом процессоре.	2	
	Практическое занятие №17. Работа с графическими объектами в текстовом процессоре.	2	
	Практическое занятие №18. Работа с графическими объектами в текстовом процессоре.	2	
Тема 2.2. Работа в редакторе электронных таблиц	**Содержание:**	**16**	
	1. Практическое занятие №19. Создание и форматирование таблицы в редакторе электронных таблиц.	2	
	2. Практическое занятие №20. Вычисление с помощью формул в электронной таблице.	2	
	3.Практическое занятие №21. Работа со встроенными функциями в электронной таблице.	2	
	4. Практическое занятие №22. Работа со списками в электронной таблице.	2	
	5. Практическое занятие №23. Создание форм для ввода данных в таблицы	2	
	6. Практическое занятие №24. Создание и работа с диаграммами и графиками.	2	
	7. Практическое занятие №25.	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	Обмен данными между текстовым процессором и электронной таблицей		
	8. Практическое занятие №26. ***Работа с расширенной фильтрацией и условным форматированием***	*2*	
Тема 2.3. Работа в программе подготовки и просмотра презентаций	Содержание:	8	
	1. Практическое занятие №27. **Построение презентации различными способами.**	2	
	2. Практическое занятие №28. **Обработка объектов слайдов презентации.**	2	
	3. Практическое занятие №29. ***Применение триггеров при создании презентации.***	*2*	
	4. Практическое занятие №30. **Настройка анимации объектов.** **Настройка показа и демонстрация результатов работы средствами мультимедиа.**	2	
Тема 2.4. Работа в системе управления базами данных	**Содержание:**	8	
	Практическое занятие №31. **Ввод данных в таблицы базы данных.**		
	Практическое занятие №32. **Создание простых запросов без параметров и с параметрами. Создание отчетов.**		
	Практическое занятие №33. ***Создание форм и их защита.***		
	4. Практическое занятие №34. ***Создание связей таблиц по типу многие-ко-многим.***		
Тема 2.5. Работа в графических редакторах	**Содержание:**	8	
	1. Практическое занятие №35. **Рисование объектов средствами графического редактора.** Работа с заливками и контурами в программе векторной графики. Работа с текстом в программе векторной графики.	2	
	2. Практическое занятие №36. **Работа с эффектами программе векторной графики.** Вставка и редактирование готового изображения с использованием программ растровой графики. Работа с цветом с использованием про-грамм растрой графики.	2	
	3. Практическое занятие №37. **Работа со спецэффектами с использованием программ растровой графики.**	2	
	4. Практическое занятие №38. ***Создание пиктограммы в графическом ре-***	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	дикторе.		
Раздел 3. Использование ресурсов технологий и сервисов Интернета		8	
Тема 3.1. Работа с ресурсами Интернета	**Содержание:**	**8**	
	1. Практическое занятие №39. Создание и обмен письмами электронной почты.	2	
	2. Практическое занятие №40. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера.	2	
	3. Практическое занятие №41. Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов.	2	
	4. Практическое занятие №42. Пересылка и публикация файлов данных в Интернете.	2	
Раздел 4. Обеспечение защиты информации в компьютерной системе		10	
Тема 4.1. Защита информации при работе с офисными приложениями	Содержание:	**10**	
	1. Практическое занятие №43. Использование штатных средств защиты операционной системы и прикладных программ.	2	
	2. Практическое занятие №44. Применение парольной защиты.	2	
	3. Практическое занятие №45. Установка антивирусных программ, их настройка. Обновление базы.	2	
	4. Практическое занятие №46. Выполнение архивирования данных.	2	
	5. Практическое занятие №47. Выполнение резервного копирования и восстановления данных	2	
Раздел 5. Организация мероприятий по обеспечению персонализированной информационной безопасности		8	
Тема 5.1. Персонализация мероприятий информационной безопасности	Содержание:	**8**	
	1. Практическое занятие №48. Выбор рациональной конфигурации оборудования в соответствии с решаемой задачей	2	

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень усвоения
	*2. **Практическое занятие №49.** **Организация работ по использованию и применению политики безопасности организации.** Организация мероприятий по резервному восстановлению данных*	2	
	*3. **Практическое занятие №50.** **Персонализация работы антивирусных программ***	2	
	*4. **Практическое занятие №51.** **Использование сервисов сети Интернет в профессиональной деятельности.** Применения программных средств для мониторинга трафика*	2	
Промежуточная аттестация в форме дифференцированного зачета		2	

IV. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к материально-техническому обеспечению

Реализация программы учебной практики предполагает наличие лабораторий:

Кабинет № 27 Лаборатория информационных технологий, программирования и баз данных

Оборудование: рабочее место преподавателя;посадочные места для обучающихся;

аудиовизуальный комплекс;комплект обучающего материала (комплект презентаций).

рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;дистрибутив устанавливаемой операционной системы;виртуальная машина для работы с операционной системой (гипервизор);СУБД;CASE-средства для проектирования базы данных;инструментальная среда программирования; пакет прикладных программ

Кабинет №23 Лаборатория Программных и программно-аппаратных средств обеспечения информационной безопасности

Оборудование: посадочных мест 30, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.Антивирусные программные комплексы, программно – аппаратные средства защиты информации от НСД, блокировка доступа и нарушения целостности, программные и программно – аппаратные средства обнаружения вторжений

Кабинет № 21 Лаборатория технических средств защиты информации; Кабинет № 21 Мастерская Лаборатория информационных технологий.

Оборудование:посадочных мест – не менее 30, рабочее место преподавателя, проектор, персональный компьютер, интерактивная доска, комплект презентаций.

Аппаратные средства аутентификации пользователя, средства защиты информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок - глушилка мобильных телефонов GPS 600- С; средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических колебаний, стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, система видеонаблюдения и охраны объектов – Подавитель Скорпион GSM+CPS, Фильтр сетевой и помехоподавляющий ФП – 6,Система видеонаблюдения ISON TOR –SE -1.

4.2. Информационное обеспечение обучения

4.2.1 Норттавно-правовые акты:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информа- ционных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регули- ровании».
4. Федеральный закон от 4 мая 20.11 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Фе- дерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Во- просы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утвер- ждении перечня сведений конфиденциального характера».
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по

обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
от 30 августа 2002 г. № 282.
16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
от 31 августа 2010 г. № 416/489.
18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК

России 10 октября 2007 г.
21. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
22. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
23. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
24. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
25. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
27. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
29. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

38.ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
39.ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
40.ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
41.ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
42.ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
43.Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
44.Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
45.ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
46.ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
47.Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России. 2002.
48.Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
49.Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
50.Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.
51.СанПиН 2.2.2/2.4.1340-03. 2.2.2. Гигиена труда, технологические процессы, сырье, материалы, оборудование, рабочий инструмент. 2.4. Гигиена детей и подростков. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы. Санитарно-эпидемиологические правила и нормативы, утв. Главным государственным

санитарным врачом РФ 30.05.2003) (Зарегистрировано в Минюсте России 10.06.2003 N 4673) // Консультант Плюс,2018
52. ТОИ Р-45-084-01. Типовая инструкция по охране труда при работе на персональном компьютере (утв. Приказом Минсвязи РФ от 02.07.2001 N 162) // Консультант Плюс, 2018

4.2.2 Основные издания:

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518005
3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/51170
4. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512423
5. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519614
6. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519614

4.2.2. Дополнительные издания:

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518006
2. Войниканис, Е. А. Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом : учебное пособие для вузов / Е. А. Войниканис ; под редакцией М. А. Федотова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 57 с. — (Высшее образование). — ISBN 978-5-534-17204-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/532605
3. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для сузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515435
4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для сузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300
5. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/51286

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

Электронные источники:

1. Информационный портал по безопасности www.SecurityLab.ru. - Текст : электронный
2. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/ - Текст : электронный
3. Сайт Научной электронной библиотеки www.elibrary.ru - Текст : электронный
4. Справочно-правовая система «Гарант» www.garant.ru - Текст : электронный
5. Справочно-правовая система «Консультант Плюс» www.consultant.ru - Текст : электронный
6. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\: www.ict.edu.ru - Текст : электронный
7. Федеральный портал «Российское образование www.edu.ru - Текст : электронный

4.3. Общие требования к организации образовательного процесса

Учебная практика проводится в учебных аудиториях и лабораториях техникума.

Учебная практика проводится преподавателями дисциплин профессионального цикла непрерывно.

Обучающиеся, совмещающие обучение с трудовой деятельностью, вправе проходить учебную практику в организации по месту работы, в случаях, если осуществляемая ими профессиональная деятельность соответствует целям практики.

4.4. Кадровое обеспечение образовательного процесса

Преподаватели, осуществляющие руководство учебной практикой обучающихся, должны иметь квалификационный разряд по профессии на 1-2 разряда выше, чем предусматривает ФГОС СПО, высшее или среднее профессиональное образование по профилю специальности, проходить обязательную стажировку в профильных организациях не реже 1-го раза в 3 года.

V. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Результаты учебной практики оцениваются преподавателем – руководителем учебной практики на основании текущего контроля в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий, выполнения проверочных практических работ с учетом представленной обучающимся отчетной документации: дневника практики, отчета, характеристики, аттестационного листа. Аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций и характеристика формируются преподавателем – руководителем учебной практики.

Учебная практика завершается дифференцированным зачетом:

- при наличии положительного аттестационного листа об уровне освоения профессиональных компетенций и положительной характеристики на обучающегося по освоению общих компетенций в период прохождения практики;
- при условии полноты и своевременности представления дневника практики и отчета по практике.

Результаты обучения в рамках ВИД:	Формы и методы контроля и оценки результатов обучения
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
Освоенные умения: – осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; – обеспечивать работоспособность, обнаруживать и устранять неисправности – *Выполнять настройку параметров работы программного обеспечения, включая системы управления-ми базами данных* – *Выполнять настройку параметров работы программного обеспечения, средства электронного документооборота*	- наблюдение за выполнением работ и экспертная оценка формирования практических профессиональных умений обучающихся на практических занятиях, в процессе учебной практики; - интерпретация результатов самостоятельной работы обучающихся на практических занятиях в процессе учебной практики; - экспертная оценка отчетов по практическим занятиям

– *Работать с программным обеспечением с соблюдением действующих требований по защите информации* – *Контролировать процесс управления учетными записями пользователей СУБД* – *Контролировать неизменность настроек средств защиты информации* – *Работать в компьютерных сетях с соблюдением действующих требований по защите информации. Конфигурация и контроль корректности настройки программно-аппаратных средств защиты информации в компьютерных сетях* – *Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях.* – *Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях* – *Разрабатывать техническое задание на создание подсистем информационной безопасности автоматизированных систем* – *Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности* – *Работать с программным обеспечением с соблюдением действующих требований по защите информации* – *Определять элементы кабельной системы, защищенные от НСД* – *Определять оптимальность выбора аппаратных средств защиты информации* – *Оценивать режимы выбора аппаратных средств защиты информации функционирования в компьютерных сетях* – *Применять программно-аппаратных средств защиты информации в компьютерных сетях* – *Настраивать правила фильтрации пакетов в компьютерных сетях* – *Определять правила фильтрации пакетов в компьютерных сетях* – *Настраивать правила фильтрации пакетов в компьютерных сетях с применение IPv4* – *Оценивать оптимальности выбора аппаратных средств защиты информации* – *Настраивать правила фильтрации пакетов и преобразование сетевых адресов* – *Настраивать правила фильтрации пакетов с использованием NAT* – *Настраивать правила фильтрации пакетов с ис-*	

пользованием скрытого NAT *– Определять предложения по применению программных средств защиты информации в компьютерных сетях* *– Определять предложения по применению программно-аппаратных средств защиты информации в компьютерных сетях* *– Настраивать правила Spanning Tree Protocol в компьютерных сетях* *– Определять правильность выбора аппаратно-программных средств защиты* *– Вносить предложения по применению средств защиты информации в режиме функционирования* *– Настраивать правила фильтрации пакетов в модели QoS* *– Управлять количеством подключаемых к портам коммутатора пользователей* *– Работать со снифферами* *– Работать со стандартом IEEE 802.1AB-2009* *– Фильтровать трафик между сетями или узлами сети* *– Фильтровать трафик на основе MAC-адресов* *– Работать с персональными межсетевыми экранами* *– Работать с правилами фильтрования с использованием NAT* *– Настраивать Сетевую Систему обнаружения вторжений* *– Настраивать Сетевую Систему обнаружения вторжений, основанной на прикладных протоколах APIDS* *– Блокировать атаки с помощью межсетевого экрана Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях*	
Приобретенный практический опыт:	- наблюдение и экспертная оценка приобретения практического опыта при выполнении работ на практических занятиях в процессе учебной практики; - интерпретация результатов дифференцированного зачета
–установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; –администрирования автоматизированных систем в защищенном исполнении; –эксплуатации компонентов систем защиты информации автоматизированных систем; –диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении *–Настройки программно-аппаратных средств защиты информации, в тома числе антивирусной защиты в*	

операционных системах по заданным шаблонам; *–Инструктажа пользователей по порядку работы в операционных системах;* *–Оформления эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах;* *–Ввода в эксплуатацию программно-аппаратных средств за щиты информации в компьютерных сетях;* *–Установки средств межсетевого экранирования в соответствии с действующими требованиями по защите информации* *–Инструктажа пользователей по порядку безопасной работы в компьютерных сетях;* *–Оформления эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях;* *–Определения состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях*	
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
Освоенные умения:	- наблюдение за выполнением работ и экспертная оценка формирования практических профессиональных умений обучающихся на практических занятиях, в процессе учебной практики; - интерпретация результатов самостоятельной работы обучающихся на практических занятиях в процессе учебной практики; - экспертная оценка отчетов по практическим занятиям
– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; – 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; – применять средства гарантированного уничтожения информации; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты 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; – *Применять нормативные документы по противодействию технической разведке* – *Применять нормативные документы для оценки уязвимости* – *Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы* – *Реализовывать правила разграничения доступа персонала к объектам доступа* – *Настраивать параметры программного обеспечения системы защиты информации автоматизированной системы* – *Работать с программой шифрования данных Kryptelite* – *Классифицировать каналы утечки информации* – *Реализовывать многоуровневую политику разграничения доступа средствами программно – аппаратного комплекса «Страж NT»* – *Определять параметры работы с Windows Registry Recovery и Registry Explorer* – *Выбирать методы защиты условно-бесплатного программного обеспечения* – *Реализовывать защитные механизмы в приложениях свободно-распространяемого ПО* – *Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации* – *Устранять известные уязвимости автоматизированной системы, приводящих к возникновению угроз безопасности информации* – *Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированной системы* – *Управлять рисками* – *Применять механизмы и службы защиты* – *Применять привилегии безопасности и доступа* – *Применять протокол SSL* – *Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем* – *Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе* – *Применять аналитические и компьютерные модели автоматизированных систем и систем защиты*	

информации *– Обеспечивать безопасность рабочих станций и серверов* *– Применять режимы работы блочных шифров, схемы кратного шифрования* *– Проводить криптоанализ алгоритмов с открытым ключом* *– Применять протоколы WPA, WEP для организации безопасного функционирования беспроводной сети* *– Подбирать оборудование для реализации проекта беспроводной сети предприятия*	
Приобретенный практический опыт:	- наблюдение и экспертная оценка приобретения практического опыта при выполнении работ на практических занятиях в процессе учебной практики; - интерпретация результатов дифференцированного зачета
–установки, настройки программных средств защиты информации в автоматизированной системе; –обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; –тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; –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; –работы с подсистемами регистрации событий; –выявления событий и инцидентов безопасности в автоматизированной системе. *–Определения правил и процедур управления системой защиты информации автоматизированной системы;* *–Определения правил и процедур выявления инцидента;* *–Определения правил и процедур реагирования на инциденты;* *–Определения правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации.* *–Определения правил и процедур управления системой защиты информации автоматизированной системы;* *–Определения правил и процедур выявления инцидента;* *–Определения правил и процедур реагирования на инциденты;* *–Определения правил и процедур защиты информа-*	

ции при выводе автоматизированной системы из эксплуатации. *–Выбора и обоснования критериев выбора эффективности функционирования защищенных автоматизированных систем;* *–Проведения экспертизы состояния защищенности информации автоматизированных систем;* *–Проведения предварительных испытаний системы защиты информации автоматизированной системы;* *–Уточнения модели угроз безопасности информации автоматизированной системы.;* *–Проведения занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне;*	
Защита информации технически средствами	
Освоенные умения: –применять технические средства для криптографической защиты информации конфиденциального характера; –применять технические средства для уничтожения информации и носителей информации; –применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; –применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; –применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; –применять инженерно-технические средства физической защиты объектов информатизации *–Оценивать защищенность ограждающих конструкций помещения от утечки информации по акустическому каналу* *–Оценивать защищенность ограждающих конструкций от утечки информации по виброакустическому каналу комплексом* *–Проводить статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении.* *–Проводить техническое обслуживание технических средств за щиты информации от утечки за счет побочных электромагнитных излучений и наводок* *–Устранять выявленные неисправности технических средств за щиты информации от утечки за счет побочных электромагнитных излучений и наводок* *–Проводить ремонт с привлечением производителей технических средств защиты информации* *–Оценивать защищенность телефонных каналов*	- наблюдение за выполнением работ и экспертная оценка формирования практических профессиональных умений обучающихся на практических занятиях, в процессе учебной практики; - интерпретация результатов самостоятельной работы обучающихся на практических занятиях в процессе учебной практики; - экспертная оценка отчетов по практическим занятиям

–Оценивать защищенность помещения от утечки информации по каналам акустоэлектрических преобразований технических средств *–Обнаруживать ПЭМИ по электрической составляющей электромагнитного поля* *–Оценивать состояние трассы наблюдения* *–Проводить испытания защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами* *–Организовывать технический контроль эффективности мер защиты информации* *–Проводить оценку разведдоступности* *–Проводить комплекс работ по проверке возможности утечки информации по техническим каналам* *–Проводить оценкузащищенности объекта информатизации* *–Разрабатывать проект системы видеонаблюдения для торговой организации* *–Настраивать системы телевизионного наблюдения с учетом специфики деятельности организации* *–Определять состав ССОИ для образовательной организации* *–Испытывать на устойчивость технические средства охраны* *–Разрабатывать проекты применения технических средств воздействия для образовательной организации* *–Изготовлять технические средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок* *–Отрабатывать конструкции технического средства защиты информации на технологичность с учетом стандартов ЕСТД* *–Проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации* *–Выполнять правила их эксплуатации средств защиты информации*	
Приобретенный практический опыт:	- наблюдение и экспертная оценка приобретения практического опыта при выполнении работ на практических занятиях в процессе учебной практики; - интерпретация результатов дифференцированного зачета
–установки, монтажа и настройки технических средств защиты информации; –технического обслуживания технических средств защиты информации; –применения основных типов технических средств защиты информации; –выявления технических каналов утечки информации; –участия в мониторинге эффективности технических средств защиты информации;	

–диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; –проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; –проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; –установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты. *–Корректировки конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки, контроля и испытаний.* *–Отработки конструкции средства защиты информации на технологичность с учетом стандартов ЕСТД;* *–Заключения договоров с поставщиками комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности* *–Сертификационных испытаний технических средств защиты информации от несанкционированного доступа на соответствие требованиям безопасности информации;* *–Испытания опытного образца защищенного технического средства обработки информации на соответствие техническим условиям.*	
Выполнение работ по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин	
Освоенные умения:	- наблюдение за выполнением работ и экспертная оценка формирования практических профессиональных умений, обучающихся на практических занятиях, в процессе учебной практики; - интерпретация результатов самостоятельной работы обучающихся на практических занятиях в процессе учебной практики; - экспертная оценка отчетов по практическим занятиям
–выполнять требования техники безопасности при работе с вычислительной техникой; –производить подключение блоков персонального компьютера и периферийных устройств; –производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; –диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; –выполнять инсталляцию системного и прикладного программного обеспечения; –создавать и управлять содержимым документов с	

помощью текстовых процессоров; –создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; –создавать и управлять содержимым презентаций с помощью редакторов презентаций; –использовать мультимедиа проектор для демонстрации презентаций; –вводить, редактировать и удалять записи в базе данных; –эффективно пользоваться запросами базы данных; –создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; –производить сканирование документов и их распознавание; –производить распечатку, копирование и тиражирование документов на принтере и других устройствах; –управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; –осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; –осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; –осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ; –осуществлять резервное копирование и восстановление данных	
Приобретенный практический опыт: –выполнения требований техники безопасности при работе с вычислительной техникой; –организации рабочего места оператора электронно-вычислительных и вычислительных машин; –подготовки оборудования компьютерной системы к работе; –инсталляции, настройки и обслуживания программного обеспечения компьютерной системы; –управления файлами; –применения офисного программного обеспечения в соответствии с прикладной задачей; –использования ресурсов локальной вычислительной сети; –использования ресурсов, технологий и сервисов Интернет; – применения средств защиты информации в компьютерной системе	- наблюдение и экспертная оценка приобретения практического опыта при выполнении работ на практических занятиях в процессе учебной практики; - интерпретация результатов дифференцированного зачета