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

РАБОЧАЯ ПРОГРАММА

ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация – техник по защите информации

2024 г.

СОДЕРЖАНИЕ

РАЗДЕЛ I. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ И ПРЕДДИПЛОМНОЙ)

1.1. Область применения программы производственной (преддипломной) практики

Программа производственной практики является составной частью программы подготовки специалистов среднего звена (ППССЗ), разработанной по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», обеспечивающей реализацию ФГОС СПО в части освоения видов 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.

1.2. Цели и задачи производственной (преддипломной) практики

Производственная практика (по профилю 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» 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 производственной 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

Целью преддипломной практики является изучение выбранного объекта для прохождения практики, исследование, сбор фактического материала для написания дипломной работы, уточнение темы дипломной работы.

Основные задачи преддипломной практики:

- использование теоретических положений для решения практических профессиональных задач;

- совершенствование умений и навыков общим и профессиональным компетенциям

Требования к результатам освоения программы производственной (преддипломной) практики

В результате освоения программы производственной 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 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.*
Обладать профессиональными компетенциями	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.

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 совершен-*

	ствованию 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*
Приобрести первоначальный практический опыт	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 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.*
Обладать профессиональными компетенциями	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.

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.*
Обладать профессиональными компетенциями	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.

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*
Обладать профессиональными компетенциями	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

1.3. Количество часов на освоение производственной практики:

Всего – 792 часов, в том числе в форме практической подготовки – 792 часа:

В рамках освоения ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении - 180 часов, в том числе в форме практической подготовки – 180 часов

В рамках освоения ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами - 216 часов, в том числе в форме практической подготовки – 216 часов

В рамках освоения ПМ.03 Защита информации техническими средствами – 144 часа, 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 - 72 часа, в том числе в форме практической подготовки – 72 часа

Преддипломная практика - 144 часа (4 недели), в том числе в форме практической подготовки – 144 часа

РАЗДЕЛ II. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

2.1 Результатом освоения программы учебной практики (по профилю специальности) 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 привер-

	женность 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

ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Тематический план производственной практики (по профилю специальности)

В рамках освоения

Код ПК	Код и наименование профессионального модуля	Количество часов по ПМ	Виды работ	Наименование тем практики	Количество часов
1	2	3	4	5	6
1.1-1.4	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	180	Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	**Тема 1.1** Эксплуатация компонентов автоматизированных (информационных) систем в защищенном исполнении	6
			Обслуживание средств защиты информации прикладного и системного программного обеспечения	**Тема 1.2** Средства защиты информации прикладного и системного программного обеспечения	6
			Настройка программного обеспечения с соблюдением требований по защите информации	**Тема 1.3** Эксплуатация программного обеспечения с соблюдением требований по защите информации	6
			Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам	**Тема 1.4** Шаблоны настройки средств антивирусной защиты	6
			Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением	**Тема 1.5** Инструктаж пользователей о соблюдении требований по защите информации	6
			Настройка встроенных средств защиты информации программного обеспечения	**Тема 1.6** Встроенные средства защиты информации программного обеспечения Windows	6
			Проверка функциони-	**Тема 1.7** Диагностика	6

			рования встроенных средств защиты информации программного обеспечения	встроенных средств защиты информации программного обеспечения Windows	
			Своевременное обнаружение признаков наличия вредоносного программного обеспечения	Тема 1.8 Обнаружение признаков наличия вредоносного программного обеспечения	6
			Обслуживание средств защиты информации в компьютерных системах и сетях	Тема 1.9 Эксплуатация средств защиты информации в компьютерных системах и сетях	6
			Обслуживание систем защиты информации в автоматизированных системах	Тема 1.10 Эксплуатация систем защиты информации в автоматизированных системах	6
			Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем	Тема 1.11 Регламентные работы по эксплуатации систем защиты информации автоматизированных систем	6
			Проверка работоспособности системы защиты информации автоматизированной системы	Тема 1.12 Система защиты информации автоматизированной системы	6
			Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	Тема 1.13 Соответствие конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	6
			Контроль стабильности характеристик системы защиты информации автоматизированной системы	Тема 1.14 Характеристики системы защиты информации автоматизированной системы	6
			Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем	Тема 1.15 Ведение технической документации, связанной с эксплуатацией систем защиты	6
			Участие в работах по обеспечению защиты информации при	Тема 1.16 Работы по обеспечению защиты информации при	6

			выводе из эксплуатации автоматизированных систем	выводе из эксплуатации автоматизированных систем	
			Настройка программно-аппаратных средств защиты информации, в том числе антивирусной защиты в операционных системах по заданным шаблонам	**Тема 1.17** Эксплуатация программно-аппаратных средств защиты информации	12
			Инструктаж пользователей по порядку работы в операционных системах	**Тема 1.18** Порядок проведения инструктажей с пользователями	6
			Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах	**Тема 1.19** Оформление документации на средства защиты информации в операционных системах	6
			Ввод в эксплуатацию программно-аппаратных средств за щиты информации в компьютерных сетях	**Тема 1.20** Порядок ввода в эксплуатацию программно-аппаратных средств за щиты информации в компьютерных сетях	12
			Установка средств межсетевого экранирования в соответствии с действующими требованиями по защите информации	**Тема 1.21** Организация установки и активации межсетевых экранов	12
			Инструктаж пользователей по порядку безопасной работы в компьютерных сетях	**Тема 1.22** Порядок проведения инструктажей с пользователями по порядку безопасной работы в компьютерных сетях	12
			Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях	**Тема 1.23** Оформление эксплуатационной документации на программно-аппаратные средства защиты информации	6
			Определение состава применяемых программно-аппаратных средств защиты информации в компь-	**Тема 1.24** Программно-аппаратные средства средства защиты информации в компьютерных сетях	12

			ютерных сетях		
			Промежуточная аттестация в форме диф. зачета		6
2.1-2.6	ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	216	Анализ принципов построения систем информационной защиты производственных подразделений	Тема 2.1 Принципы построения систем информационной защиты производственных подразделений	18
			Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы	Тема 2.2 Эксплуатация элементов программной и аппаратной защиты автоматизированной системы	18
			Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности	Тема 2.3 Организация диагностики работоспособности программно-аппаратных средств обеспечения информационной безопасности	18
			Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	Тема 2.4 Эффективность использования программно-аппаратных средств обеспечения информационной безопасности	18
			Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	Тема 2.5 Организация документооборота конфиденциальной информации	12
			Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики	Тема 2.6 Нормативно-правовая база по обеспечению информационной безопасности программно-аппаратными средствами	12
			Определение правил и процедур управления системой защиты информации автома-	Тема 2.7 Правила и процедуры управления системой защиты информации автома-	12

			тизированной системы	тизированной системы	
			Определение правил и процедур выявления инцидента	**Тема 2.8** Правила и процедуры выявления инцидента	12
			Определение правил и процедур реагирования на инциденты	**Тема 2.9** Правила и процедуры реагирования на инциденты	12
			Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации	**Тема 2. 10** Правила и процедуры защиты информации при выводе автоматизированной системы из эксплуатации	12
			Выбор и обоснование критериев выбора эффективности функционирования защищенных автоматизированных систем	**Тема 2.11** Критерии выбора эффективности функционирования защищенных автоматизированных систем	12
			Проведение экспертизы состояния защищенности информации автоматизированных систем	**Тема 2.12** Оценка состояния защищенности информации автоматизированных систем	12
			Проведение предварительных испытаний системы защиты информации автоматизированной системы	**Тема 2.13** Предварительные испытания системы защиты информации автоматизированной	12
			Уточнение модели угроз безопасности информации автоматизированной системы	**Тема 2.14** Модели угроз безопасности информации автоматизированной системы	12
			Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне	**Тема 2.15** Организация занятий с персоналом по работе с системой защиты информации автоматизированной системы	18
			Промежуточная аттестация в форме диф. зачета		6
3.1-3.5	ПМ.03 Защита информации техническими средствами	144	Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации	**Тема 3.1** Монтаж и эксплуатация технических средств защиты информации	18

			Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения	Тема 3.2 Монтаж и эксплуатация средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения	18
			Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам	Тема 3.3 Монтаж и эксплуатация средств защиты информации от несанкционированного съёма и утечки по техническим каналам	18
			Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами	Тема 3.4 Нормативно-правовая база по обеспечению защиты информации техническими средствами	18
			Корректировка конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки, контроля и испытаний	Тема 3.5 Конструкторская документация на изготовление средства защиты информации от несанкционированного доступа	18
			Отработка конструкции средства защиты информации на технологичность с учетом стандартов ЕСТД	Тема 3.6 Технологичность конструкции средства защиты информации	12
			Заключение договоров с поставщиками комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности	Тема 3.7 Оформление и заключение договоров с поставщиками комплектующих изделий и материалов и лицензионных соглашений	12
			Сертификационные испытания технических средств защиты	Тема 3.8 Сертификация технических средств защиты	12

			информации от несанкционированного доступа на соответствие требованиям безопасности информации	информации от несанкционированного доступа	
			Испытания опытного образца защищенного технического средства обработки информации на соответствие техническим условиям	**Тема 3.9** Проведение испытаний образцов технического средства обработки информации	12
			Промежуточная аттестация в форме диф. зачета		6
4.1-4.4	ПМ.04 Выполнение работ по профессии рабочего 16199 Оператор электронно - вычислительных и вычислительных машин	72	Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения	**Тема 4.1.** Подготовка оборудования компьютерной системы к работе.	6
				Тема 4.2. Инсталляция и настройка системного и прикладного программного обеспечения.	6
				Тема 4.3. Установка и замена расходных материалов. Диагностика простейших неисправностей ПК, периферийного оборудования и компьютерной оргтехники.	6
			Ознакомление с документацией. Создание и управление текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах	**Тема 4.4.** Создание документов с помощью текстовых процессоров	6
				Тема 4.5. Создание документов с помощью редакторов таблиц	6
				Тема 4.6. Создание деловой презентации, в том числе бизнес презентации	6
				Тема 4.7. Работа с базами данных организации, работа с графическими редакторами.	6
			Использование	**Тема 4.8.** Структура и	6

			ресурсов локальных вычислительных сетей, ресурсов технологий и сервисов Интернета	принцип работы локальной вычислительной сети организации	
				Тема 4.9. Использование ресурсов технологий и сервисов Интернета.	6
			Применение средств защиты информации в компьютерной системе	Тема 4.10. Антивирусная защита персонального компьютера	6
				Тема 4.11. Резервное копирование и восстановление данных	6
			Промежуточная аттестация в форме диф. зачета		6
	Всего часов				756

Содержание производственной практики (по профилю специальности)

Содержание производственной практики (по профилю специальности) определяется требованиями к умениям и практическому опыту в рамках модулей ППССЗ 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,, предусмотренных ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	**Содержание видов работ**	Объем часов	Уровень освоения
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		180	
Виды работ: Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации Обслуживание средств защиты информации прикладного и системного программного			

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
обеспечения Настройка программного обеспечения с соблюдением требований по защите информации Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением Настройка встроенных средств защиты информации программного обеспечения Проверка функционирования встроенных средств защиты информации программного обеспечения Своевременное обнаружение признаков наличия вредоносного программного обеспечения Обслуживание средств защиты информации в компьютерных системах и сетях Обслуживание систем защиты информации в автоматизированных системах Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем Проверка работоспособности системы защиты информации автоматизированной системы Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации Контроль стабильности характеристик системы защиты информации автоматизированной системы Ведение технической документации, связанной с эксплуатаци-			

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
ей систем защиты информации автоматизированных систем Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем *Настройка программно-аппаратных средств защиты информации, в том 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 защиты информации в компьютерных сетях* *Установка средств межсетевого экранирования в соответствии с действующими требованиями по защите информации* *Инструктаж пользователей по порядку безопасной работы в компьютерных сетях* *Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях* *Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях*			
Тема 1.1. Эксплуатация компонентов автоматизированных (информационных) систем в защищенном исполнении	**Содержание:**	6	
	Установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатацион-		2

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
	ной документации		
Тема 1.2. Средства защиты информации прикладного и системного программного обеспечения	**Содержание:**	**6**	
	Обслуживание средств защиты информации прикладного и системного программного обеспечения		2
Тема 1.3. Эксплуатация программного обеспечения с соблюдением требований по защите информации	Содержание:	6	
	Настройка программного обеспечения с соблюдением требований по защите информации		2
Тема 1.4. Шаблоны настройки средств антивирусной защиты	Содержание:	6	
	Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам		2
Тема 1.5. Инструктаж пользователей о соблюдении требований по защите информации	Содержание:	6	
	Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением		2
Тема 1.6. Встроенные средства защиты информации программного обеспечения Windows	Содержание:	6	
	Настройка встроенных средств защиты информации программного обеспечения		2
Тема 1.7. Диагностика встроенных средств защиты информации программного обеспечения Windows	Содержание:	6	
	Проверка функционирования встроенных средств защиты информации программного обеспечения		2
Тема 1.8. Обнаружение признаков наличия вредоносного программного обеспечения	Содержание:	6	
	Своевременное обнаружение признаков наличия вредоносного программного обеспечения		2
Тема 1.9. Эксплуатация средств защиты информации в компьютерных системах и сетях	Содержание:	6	
	Обслуживание средств защиты информации в компьютерных системах и сетях		2
Тема 1.10 Эксплуатация систем защиты информации в автоматизированных системах	Содержание:	6	
	Обслуживание систем защиты информации в автоматизированных системах		2
Тема 1.11 Регламентные работы по эксплуатации систем защиты	Содержание:	6	
	Участие в проведении регла-		2

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
информации автоматизированных систем	ментных работ по эксплуатации систем защиты информации автоматизированных систем		
Тема 1.12 Система защиты информации автоматизированной системы	**Содержание:**	6	
	Проверка работоспособности системы защиты информации автоматизированной системы		2
Тема 1.13 Соответствие конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	**Содержание:**	6	
	Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации		2
Тема 1.14 Характеристики системы защиты информации автоматизированной системы	**Содержание:**	6	
	Контроль стабильности характеристик системы защиты информации автоматизированной системы		2
Тема 1.15 Ведение технической документации, связанной с эксплуатацией систем защиты	**Содержание:**	6	
	Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем		2
Тема 1.16 Работы по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	**Содержание:**	6	
	Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем		2
Тема 1.17 Эксплуатация программно-аппаратных средств защиты информации	**Содержание:**	12	
	Настройка программно-аппаратных средств защиты информации, в том числе антивирусной защиты в операционных системах по заданным шаблонам		2
Тема 1.18 Порядок проведения инструктажей с пользователями	**Содержание:**	6	
	Инструктаж пользователей по порядку работы в операционных системах		2
Тема 1.19 Оформление документации на средства защиты информации в операционных системах	**Содержание:**	6	
	Оформление эксплуатационной документации на программно- аппаратные средства защиты информации		2

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
	в операционных системах		
Тема 1.20 Порядок ввода в эксплуатацию программно-аппаратных средств за щиты информации в компьютерных сетях	**Содержание:**	12	
	Ввод в эксплуатацию программно-аппаратных средств за щиты информации в компьютерных сетях		2
Тема 1.21 Организация установки и активации межсетевых экранов	**Содержание:**	12	
	Установка средств межсетевого экранирования в соответствии с действующими требованиями по защите информации		2
Тема 1.22 Порядок проведения инструктажей с пользователями по порядку безопасной работы в компьютерных сетях	**Содержание:**	12	
	Инструктаж пользователей по порядку безопасной работы в компьютерных сетях		2
Тема 1.23 Оформление эксплуатационной документации на программно-аппаратные средства защиты информации	**Содержание:**	6	
	Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях		2
Тема 1.24 Программно-аппаратные средства средства защиты информации в компьютерных сетях	Содержание:	12	
	Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях		2
Промежуточная аттестация в форме дифференцированного зачета		6	
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		**216**	
Анализ принципов построения систем информационной защиты производственных подразделений Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств			

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
обеспечения информационной безопасности Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики *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* *Выбор и обоснование критериев выбора эффективности функционирования защищенных автоматизированных систем* *Проведение экспертизы состояния защищенности информации автоматизированных систем* *Проведение предварительных испытаний системы защиты информации автоматизированной системы* *Уточнение модели угроз*			

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
безопасности информации автоматизированной системы Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне			
Тема 2.1. Принципы построения систем информационной защиты производственных подразделений	**Содержание:**	**18**	
	Инструктаж по ОТ и ТБ в подразделении защиты информации		2
	Принципы построения систем информационной защиты производственных подразделений		2
	Анализ принципов построения систем информационной защиты производственных подразделений		2
Тема 2.2. Эксплуатация элементов программной и аппаратной защиты автоматизированной системы	**Содержание:**	**18**	
	Определение состава элементов программной и аппаратной защиты автоматизированной системы		2
	Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы		2
	Документирование эксплуатации системы защиты автоматизированной системы		2
Тема 2.3. Организации диагностики работоспособности программно-аппаратных средств обеспечения информационной безопасности	**Содержание:**	**18**	
	Участие в диагностировании программно-аппаратных средств обеспечения информационной безопасности		2
	Участие в устранении отказов программно-аппаратных средств обеспечения информационной безопасности		2
	Участие в обеспечении работоспособности программно-аппаратных средств		2

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
	обеспечения информационной безопасности		
Тема 2.4. Эффективность использования программно-аппаратных средств обеспечения информационной безопасности	**Содержание:**	18	
	Определение состава программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении		2
	Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении		2
	Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении		2
Тема 2.5. Организация документооборота конфиденциальной информации	**Содержание:**	12	
	Участие в обеспечении учета и обработки конфиденциальной информации		2
	Участие в процессах хранения и передачи конфиденциальной информации		2
Тема 2.6. Нормативно-правовая база по обеспечению информационной безопасности программно-аппаратными средствами	**Содержание:**	12	
	Применение нормативных правовых актов по обеспечению информационной безопасности программно-аппаратными средствами при работе в структурном подразделении		2
	Применение нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики		2
Тема 2.7. Правила и процедуры управления системой защиты информации автоматизированной системы	**Содержание:**	12	
	Определение правил управления системой защиты информации автоматизированной системы		2
	Определение процедур управ-		2

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
	ления системой защиты информации автоматизированной системы		
Тема 2.8. Правила и процедуры выявления инцидента	**Содержание:**	**12**	
	Определение правил выявления инцидента		2
	Определение процедур выявления инцидента		2
Тема 2.9. Правила и процедуры реагирования на инциденты	**Содержание:**	**12**	
	Определение правил реагирования на инциденты		2
	Определение процедур реагирования на инциденты		2
Тема 2.10 Правила и процедуры защиты информации при выводе автоматизированной системы из эксплуатации	**Содержание:**	**12**	
	Определение правил защиты информации при выводе автоматизированной системы из эксплуатации		2
	Определение процедур защиты информации при выводе автоматизированной системы из эксплуатации		2
Тема 2.11 Критерии выбора эффективности функционирования защищенных автоматизированных систем	**Содержание:**	**12**	
	Выбор и обоснование критериев выбора эффективности функционирования защищенных автоматизированных систем		2
	Оценка эффективности функционирования защищенных автоматизированных систем		2
Тема 2.12 Оценка состояния защищенности информации автоматизированных систем	**Содержание:**	**12**	
	Проведение экспертизы состояния защищенности информации автоматизированных систем		2
	Документирование результатов экспертизы		2
Тема 2.13 Предварительные испытания системы защиты информации автоматизированной	**Содержание:**	**12**	
	Проведение предварительных испытаний системы защиты информации автоматизированной системы		2
	Документирование результатов испытаний		2

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
Тема 2.14 Модели угроз безопасности информации автоматизированной системы	**Содержание:**	12	
	Уточнение модели угроз безопасности информации автоматизированной системы		2
	Разработка раздела политики информационной безопасности		2
Тема 2.15 Организация занятий с персоналом по работе с системой защиты информации автоматизированной системы	**Содержание:**	18	
	Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы		2
	Проведение практических занятий с персоналом в тестовой зоне		2
	Отработка ситуационных задач		2
Промежуточная аттестация в форме дифференцированного зачета		6	
ПМ.03 Защита информации техническими средствами		144	
Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами *Корректировка конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки, кон-*			

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
троля 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* *Сертификационные испытания технических средств защиты информации от несанкционированного доступа на соответствие требованиям безопасности информации* *Испытания опытного образца защищенного технического средства обработки информации на соответствие техническим условиям*			
Тема 3.1 Монтаж и эксплуатация технических средств защиты информации	**Содержание:**	18	
	Участие в монтаже технических средств защиты информации		2
	Участие в обслуживании технических средств защиты информации		2
	Участие в эксплуатации технических средств защиты информации		2
Тема 3.2 Монтаж и эксплуатация средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения	**Содержание:**	18	
	Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности.		2
	Участие в монтаже, обслуживании и эксплуатации средств инженерной защиты и технической охраны объектов		2
	Участие в монтаже, обслуживании и эксплуатации систем видеонаблюдения		2
Тема 3.3 Монтаж и эксплуатация средств защиты информа-	Содержание:	18	
	Участие в монтаже средств		2

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
ции от несанкционированного съёма и утечки по техническим каналам	защиты информации от несанкционированного съёма и утечки по техническим каналам		
	Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам		2
	Участие в эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам		2
Тема 3.4 Нормативно-правовая база по обеспечению защиты информации техническими средствами	**Содержание:**	18	
	Применение нормативно правовых актов по обеспечению защиты информации техническими средствами		2
	Применение нормативных методических документов по обеспечению защиты информации техническими средствами		2
	Документирование процедуры аудита на соответствие нормативной базе		2
Тема 3.5 Конструкторская документация на изготовление средства защиты информации от несанкционированного доступа	**Содержание:**	18	
	Корректировка конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки		2
	Корректировка конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для контроля		2
	Корректировка конструкторской документации на изготовление средства защиты информации от несанкционированного доступа испытаний		2
Тема 3.6 Технологичность конструкции средства защиты	**Содержание:**	12	
	Отработка конструкции		2

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
информации	*средства защиты информации на технологичность с учетом стандартов ЕСТД*		
	Подготовка пакета документов на средство защиты информации		2
Тема 3.7 Оформление и заключение договоров с поставщиками комплектующих изделий и материалов и лицензионных соглашений	**Содержание:**	12	
	Участие в заключении договоров с поставщиками комплектующих изделий и материалов		2
	Участие в заключении договоров с правообладателями на использование объектов промышленной и интеллектуальной собственности		2
Тема 3.8 Сертификация технических средств защиты информации от несанкционированного доступа	**Содержание:**	12	
	Участие в сертификационных испытаниях технических средств защиты информации от несанкционированного доступа на соответствие требованиям безопасности информации		2
	Документирование процедуры сертификационных испытаний		2
Тема 3.9 Проведение испытаний образцов технического средства обработки информации	Содержание:	12	
	Участие в испытаниях опытного образца защищенного технического средства обработки информации на соответствие техническим условиям		2
	Документирование процедуры испытаниях опытного образца		2
Промежуточная аттестация в форме дифференцированного зачета		6	
ПМ. 04. Выполнение работ по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин, в том числе профессиональными (ПК) и общими (ОК) компетенциями		72	
Виды работ: Ознакомление с персональным компьютером. Выполнение настройки интерфейса операци-			

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
онной системы. Управление файлами данных на локальных, съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в Интернете. Подключение периферийных устройств и компьютерной оргтехники к персональному компьютеру и настройка режимов ее работы. Распечатка, копирование и тиражирование документов на принтере и других периферийных устройствах вывода. Осуществление резервного копирования и восстановления данных. Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники Создание и управление содержимым документов с помощью редактора документов; таблиц с помощью редакторов таблиц; презентаций с помощью редакторов презентаций. Обработка графической информации средствами графических программ. Распознавание сканированных текстовых документов с помощью программ распознавания текста. Создание и обмен письмами электронной почты. Поиск, сортировка и анализ информации с помощью поисковых интернет-сайтов; пересылка и публикация файлов данных в Интернете. Организация антивирусной защиты персонального компьютера с помощью антивирусных программ; ведение отчетной и технической документации.			

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
Тема 4.1. Подготовка оборудования компьютерной системы к работе	**Содержание:**	6	
	Техника безопасности при работе с вычислительной техникой: *изучение нормативной документации.* Организация рабочего места оператора электронно-вычислительных и вычислительных машин: *учёт антропометрических данных, выбор рациональной рабочей поверхности, физиологически рациональной рабочей позы, оргтехоснастка, защита от блесткости.*		2
	Подключение блоков персонального компьютера и периферийных устройств: *конструктивы (разъемы), основные характеристики*		2
	Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка		2
Тема 4.2. Инсталляция и настройка системного и прикладного программного обеспечения.	**Содержание:**	6	
	Установка операционной системы, настройка интерфейса ОС: *специальные возможности и дополнительные параметры*		2
	Инсталляция прикладного программного обеспечения: *особенности специализированного прикладного программного обеспечения*		2
	Настройка системного и прикладного программного обеспечения в соответствии с прикладной задачей.		2
Тема 4.3. Установка и замена расходных материалов. Диагностика простейших неисправностей ПК, периферийного оборудования и компьютерной оргтехники.	**Содержание:**	6	
	Установка и замена расходных материалов для принтеров, ксерокса, плоттера.		2
	Диагностика простейших неисправностей ПК: *блок питания; материнская плата;*		2

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
	оперативная память; видеокарта; центральный процессор; конденсаторы		
	Диагностика простейших неисправностей периферийного оборудования и компьютерной оргтехники: *выявление устройств, вышедших из строя, и подбор для них подходящей замены.*		2
Тема 4.4. Создание документов с помощью текстовых процессоров. Управление документами.	**Содержание:**	6	
	Создание текстовых документов: *создание документов с помощью шаблонов и форм.*		2
	Сканирование документов и их распознавание: *сканирование прозрачных и непрозрачных оригиналов.*		2
	Распечатка, копирование и тиражирование документов на принтере и других устройствах: произведение копирования документов на различные съемные носители: *установка современных приложений беспроводной передачи данных для их последующей печати.*		2
Тема 4.5. Создание документов с помощью редакторов таблиц	**Содержание:**	6	
	Создание и редактирование документов организации с применением ЭТ: *экспресс-анализ, использование срезов для фильтрации данных*		2
	Обмен данными между текстовым процессором и электронной таблицей в документе: *внедрение данных листа в веб-страницу, обмен листами Excel в онлайн-встрече*		2
	Использование возможностей		2

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
	ЭТ по поиску решения: *создание подходящей сводной таблицы, использование нескольких таблиц при анализе данных.*		
Тема 4.6. Создание деловой презентации, в том числе бизнес презентации	**Содержание:**	6	
	Создание презентации с применением триггеров: конструктор в PowerPoint		2
	Создание деловой анимированной презентации: *создание переходов кинематографического уровня с Трансформацией*		2
	Создание бизнес презентации с эффектами анимации. Демонстрация презентации.		2
Тема 4.7. Работа с базами данных организации, работа с графическими редакторами.	**Содержание:**	6	
	1. Базы данных организации: *создание, заполнение, форматирование. Составление сложных запросов баз данных. Фильтрация данных.*		2
	2. *Создание форм и отчётов с помощью мастера форм базы данных.*		2
	3. *Создание пиктограммы в рамках деятельности организации*		2
Тема 4.8. Структура и принцип работы локальной вычислительной сети организации	**Содержание:**	6	
	Структура локальной вычислительной сети организации: топология, протоколы, распределение ресурсов и прав доступа		2
	Принцип работы локальной вычислительной сети организации. Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети		2
	Диагностика и устранение простейших неисправностей при работе в компьютерной		2

Код и наименование профессиональных модулей и тем производственной практики по профилю специальности	Содержание видов работ	Объем часов	Уровень освоения
	сети.		
Тема 4.9. Использование ресурсов технологий и сервисов	**Содержание:**	6	
	Навигация по Веб-ресурсам Интернета с помощью браузера: *загрузка документа, чтение страницы, переход по гиперссылкам, просмотр html-кода.*		2
	Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов.		2
	Настройка параметров ящика электронной почты организации. Создание и обмен письмами электронной почты.		2
Тема 4.10. Антивирусная защита персонального компьютера	**Содержание:**	6	
	1. Антивирусная защита персонального компьютера с помощью антивирусных программ: *настройка брандмауэра, проверка файлов в ручном режиме*		2
	2. *Организация работ по использованию и применению политики безопасности организации*		2
	3. *Персонализация работы антивирусных программ*		2
Тема 4.11. Резервное копирование и восстановление данных	**Содержание:**	6	
	1. Осуществление резервного копирования и восстановления данных: *применение облачных сервисов и Drive Backup*		2
	2. *Организация мероприятий по резервному восстановлению данных*		2
	3. *Использование сервисов сети Интернет в деятельности организации. Применение программных средств для мониторинга трафика*		2
Промежуточная аттестация в форме дифференцированного зачета		6	

4. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Место прохождения производственной практики (по профилю специальности)

Реализация программы производственной практики (по профилю специальности) осуществляется в условиях реального производственного процесса в организациях, направление деятельности которых соответствует профилю подготовки обучающихся на основе договоров, заключаемых между техникумом и организациями.

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

Требования к документации, необходимой для проведения практики

- Рабочая программа производственной практики
- Календарно тематический план.
- Нормативные документы по обеспечению производственной практики
- График проведения производственной практики.
- График консультаций.
- График защиты отчётов по практике

Требования к учебно-методическому и материально-техническому обеспечению производственной практики

Оборудование и технологическое оснащение рабочих мест при прохождении производственной практики (по профилю специальности): рабочее место должно быть оборудовано комплектом нормативных актов и методических документов, компьютерной техникой с программным обеспечением общего и профессионального назначения, оргтехникой, средствами защиты информации и сетевым оборудованием.

4.2. Информационное обеспечение обучения

4.2.1 Нормативно-правовые акты:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных 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 регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдель-

ных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении 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

4.2.3. 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.

4.2.4 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

Общие требования к организации образовательного процесса

Организацию и руководство практикой (по профилю специальности) осуществляют руководители практики техникума и от организации на основании программы производственной практики (по профилю специальности) и календарно-тематического плана.

В период прохождения производственной практики (по профилю специальности) обучающиеся могут зачисляться на вакантные должности, если работа соответствует требованиям программы производственной практики.

Обучающиеся в период прохождения производственной практики (по профилю специальности) в организациях, обязаны:

- выполнять задания, предусмотренные программами практики в соответствии с разделами календарно-тематического плана прохождения практики и индивидуальные задания;
- соблюдать действующие в организациях правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности.

Производственная практика (по профилю специальности) проводится непрерывно в рамках профессиональных модулей.

Кадровое обеспечение образовательного процесса

Руководителями практики (по профилю специальности) от техникума являются преподаватели дисциплин профессионального цикла.

КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Контроль и оценка результатов освоения практики (по профилю специальности) осуществляется руководителем практики от техникума и от организации в процессе прохождения студентами практики.

Текущий контроль производственной практики (по профилю специальности) осуществляется на основе разработанного графика целевых проверок, в котором указаны сроки и фамилии проверяющих.

Качество контроля практики обеспечивается планомерностью проверок производственной деятельности практикантов, проведением своевременных консультаций, оказанием методической помощи.

Руководитель практики от техникума контролирует реализацию программы и условия проведения практики организациями, в том числе требования охраны труда, безопасности жизнедеятельности и пожарной безопасности в соответствии с правилами и нормами, в том числе отраслевыми.

Оценка результатов освоения производственной практики (по профилю специальности)

Аттестация обучающихся по итогам производственной практики (по профилю специальности) проводится на основании представленной обучающимся отчетной документации: дневника практики, отчета, характеристики, аттестационного листа в соответствии с заданием на практику.

По результатам практики руководителями практики от организации и от техникума формируется аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций, а также характеристика на обучающегося по освоению общих компетенций в период прохождения практики.

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 в соответствии с заданием на практику.

Работа над отчетом по практике должна позволить руководителю оценить уровень развития общих компетенций студента. Текст отчета должен быть подготовлен с использованием компьютера в Word, распечатан на одной стороне белой бумаги формата А4 (210х297 мм). Цвет шрифта - черный, межстрочный интервал - полуторный, гарнитура - Times New Roman, размер шрифта - 14 кегль.

Результаты обучения в рамках ВПД: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	**Формы и методы контроля и оценки результатов обучения**
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 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 безопас-*	Наблюдение за выполнением работ и экспертная оценка формирования практических профессиональных умений, практического опыта, общих и профессиональных компетенций обучающихся в период практики (по профилю специальности) Аттестационный лист о прохождении практики (по профилю специальности) Характеристика руководителя практики (по профилю специальности) Отчет по практике Интерпретация результатов практики (по профилю специальности) на основе документов соответствующих организаций

ности 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*	
Приобретенный 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 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*	
Профессиональные компетенции:	
–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	
Результаты обучения в рамках ВПД: Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Формы и методы контроля и оценки результатов обучения
Освоенные умения:	Наблюдение за выполнением работ и экспертная оценка формирования практических профессиональных умений, практического опыта, общих и профессиональных компетенций обучающихся в период практики (по профилю специальности) Аттестационный лист о прохождении практики (по профилю специальности) Характеристика руководителя практики (по профилю специальности) Отчет по практике Интерпретация результатов практики (по профилю специальности) на основе документов соответствующих организаций
– 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:	
–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 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;*	
Профессиональные компетенции:	
–ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. –ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. –ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. –ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. –ПК 2.5. Уничтожать информацию и носители информации с использованием программных и	

программно-аппаратных средств. –ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	
Результаты обучения в рамках ВПД: Защита информации технически средствами	Формы и методы контроля и оценки результатов обучения
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, практического опыта, общих и профессиональных компетенций обучающихся в период практики (по профилю специальности) Аттестационный лист о прохождении практики (по профилю специальности) Характеристика руководителя практики (по профилю специальности) Отчет по практике Интерпретация результатов практики (по профилю специальности) на основе документов соответствующих организаций

–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:	
–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.*	
Профессиональные компетенции:	
- 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.	
Результаты обучения в рамках ВПД: Выполнение работ по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин	**Формы и методы контроля и оценки результатов обучения**
Освоенные умения: - выполнять требования техники безопасности при работе с вычислительной техникой: выполнять требования нормативной документации; - производить подключение блоков персонального компьютера и периферийных устройств: конструктивы (разъемы), основные характеристики; - работать с дополнительными внешними устройствами ПК - производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; - диагностировать простейшие неисправности персонального компьютера: блок питания; материнская плата; оперативная память; видеокарта; центральный процессор; конденсаторы, периферийного оборудования и компьютерной оргтехники; выявление устройств, выпедших из строя, и подбор для них подходящей замены - выполнять инсталляцию системного и прикладного программного обеспечения; - использовать специальные возможности и дополнительные параметры ОС, особенности специализированного прикладного программного обеспечения;	Наблюдение за выполнением работ и экспертная оценка формирования практических профессиональных умений, практического опыта, общих и профессиональных компетенций обучающихся в период практики (по профилю специальности) Аттестационный лист о прохождении практики (по профилю специальности) Характеристика руководителя практики (по профилю специальности) Отчет по практике Интерпретация результатов практики (по профилю специальности) на основе документов соответствующих организаций

- настраивать системное и прикладное программного обеспечения в соответствии с прикладной задачей. - создавать и управлять содержимым документов с помощью текстовых процессоров: создание документов с помощью шаблонов и форм; - создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц: экспресс-анализ, использование срезов для фильтрации данных, внедрение данных листа в веб-страницу, обмен листами Excel в онлайн-встрече, создание подходящей сводной таблицы, использование нескольких таблиц при анализе данных. - использовать мультимедиа проектор для демонстрации презентаций: создание переходов кинематографического уровня с Трансформацией - вводить, редактировать и удалять записи в базе данных; - эффективно пользоваться запросами базы данных; - составлять сложные запросы; - создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики: создание пиктограммы в рамках деятельности организации; - производить сканирование документов и их распознавание: сканирование прозрачных и непрозрачных оригиналов; - производить распечатку, копирование и тиражирование документов на принтере и других устройствах: установка современных приложений беспроводной передачи данных для их последующей печати; - определять структуру локальной вычислительной сети организации: топологию, протоколы, распределение ресурсов и прав доступа - 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: загрузка документа, чтение страницы, переход по гиперссылкам, просмотр html-кода. - осуществлять диагностику и устранение простейших неисправностей при работе в компьютерной сети	

- осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; - осуществлять настройку параметров ящика электронной почты организации. Создавать и обмениваться письмами электронной почты. - осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ: настройка брандмауэра, проверка файлов в ручном режиме; - осуществлять резервное копирование и восстановление данных: применение облачных сервисов и Drive Backup	
Приобретенный практический опыт:	
– выполнения требований техники безопасности при работе с вычислительной техникой: *выполнения требований нормативной документации*; – организации рабочего места оператора электронно-вычислительных и вычислительных машин: *учёт антропометрических данных, выбор рациональной рабочей поверхности, физиологически рациональной рабочей позы, оргтехоснастка, защита от блесткости*; – подготовки оборудования компьютерной системы к работе; – инсталляции, настройки и обслуживания программного обеспечения компьютерной системы: *особенности специализированного прикладного программного обеспечения*; – управления файлами; – применения офисного программного обеспечения в соответствии с прикладной задачей; – использования ресурсов локальной вычислительной сети: *топология, протоколы, распределение ресурсов и прав доступа*; – использования ресурсов, технологий и сервисов Интернет; – применения средств защиты информации в компьютерной системе. – *создания форм и их защиты.* – *работы с расширенной фильтрацией и условным форматированием* – *применения триггеров при создании презентации* – *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*	
Профессиональные компетенции:	
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	

РАЗДЕЛ III. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Результатом освоения программы преддипломной практики является сформированность у студентов общих и профессиональных компетенций, углубление первоначального практического опыта и реализуется в рамках модулей ППСЗ 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).

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

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

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 самоуправле-

	нии, 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

ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Преддипломная практика включает сбор и предварительную обработку материалов, необходимых для написания дипломной работы.

Материалы, собранные во время практики должны включать теоретическую информацию о предмете исследования, практическую исходную информацию, её предварительный анализ.

Конкретное содержание собранных в процессе преддипломной практики материалов зависит от темы дипломной работы.

№ п/п	Наименование видов работ	Количество часов на вид работы
1	Общее ознакомление с историей и работой организации. Работа с должностными инструкциями отдела защиты информации. Изучение нормативно-правовой и эксплуатационной документации на системы и средства защиты информации, применяемые в организации.	12
2	Ведение текущей работы исполнителей с конфиденциальной информацией	12
3	Организация охраны персонала, территорий, зданий, помещений и продукции организаций. Использование аппаратуры систем контроля доступа	6
4	**Работа над дипломной работой** 2.1 Изучение и сбор информации и практического материала для дипломной работы 2.2 Сбор материала для дипломной работы 2.3 Сбор приложений для дипломной работы	102 36 36 30
5	**Составление отчетной документации по производственной (преддипломной) практике**	12
	Итого	144

УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Место прохождения производственной (преддипломной) практики

Реализация программы преддипломной практики осуществляется в организациях на основе договоров, заключаемых между образовательным учреждением и этими организациями. Студенты, заключившие договоры с будущими работодателями, могут проходить практику в этих организациях. При наличии вакантных должностей студенты могут зачисляться на них, если работа соответствует требованиям программы практики.

Студенты заочной формы обучения, как правило, самостоятельно определяют место прохождения преддипломной практики. Оформление необходимых для этого документов производится в соответствии с установленным в учебном заведении порядком.

Для прохождения практики студенту предоставляется право выбора организации для прохождения практики. Это могут быть организации всех форм собственности, имеющие службы, отделы или группы информационной безопасности, защиты информации:

- органы власти и управления субъектов РФ (города, района и т. п.);
- государственные организации;
- муниципальные организации;
- образовательные учреждения;
- акционерные общества;
- частные организации;
- государственные архивы;
- кадровые агентства;

Организация как база практики должна:

- иметь сферы деятельности, предусмотренные программой практики;
- располагать квалифицированными кадрами для руководства практикой.

Требования к материально-техническому обеспечению

Организации, участвующие в проведении практики, предоставляют рабочие места практикантам, обеспечивают безопасные условия прохождения практики, отвечающие санитарным правилам и требованиям охраны труда; проводят инструктаж по ознакомлению с требованиями охраны труда и техники безопасности в организации.

Оборудование и технологическое оснащение рабочих мест при прохождении преддипломной практики: рабочее место должно быть оборудовано компьютерной техникой с программным обеспечением профессионального назначения.

4.2. Информационное обеспечение обучения

4.2.1 Нормативно-правовые акты:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных 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 регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении 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 конфи-

денциальной 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. Факто-

ры, 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

4.2.3. 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

Общие требования к организации образовательного процесса

Организацию и руководство преддипломной практикой осуществляют руководители практики от техникума и от организации на основании программы преддипломной практики и календарно - тематического плана.

Руководитель дипломной работы определяет общую схему изучения объекта исследования, дает рекомендации по литературе и консультирует студента в период прохождения практики.

Руководители практики от техникума составляют графики посещения мест практики, устанавливают связь с руководителями практики от предприятий и совместно с ними составляют программу проведения практики, разрабатывают тематику индивидуальных заданий, принимают участие в распределении студентов по рабочим местам или перемещений их по видам работ, осуществляют контроль за правильностью использования студентов в период практики, оказывают методическую помощь студентам при выполнении ими индивидуальных заданий и сбору материалов к дипломной работе, организовывают процедуру оценки общих и

профессиональных компетенций студента, освоенных им в ходе прохождения практики; разрабатывают и согласовывают с организациями формы отчетности и оценочный материал прохождения практики.

Руководитель преддипломной практики, назначенный в организации, где студент проходит практику, обеспечивает предоставление студенту необходимой информации и условий для исследования, участвует в организации и оценке результатов освоения общих и профессиональных компетенций, полученных в период прохождения практики; участвует в формировании оценочного материала для оценки общих и профессиональных компетенций, освоенных студентами в период прохождения практики; обеспечивает безопасные условия прохождения практики, отвечающие санитарным правилам и требованиям охраны труда; проводит инструктаж по ознакомлению с требованиями охраны труда и техники безопасности в организации, а также устанавливает регламент работ студента.

Кадровое обеспечение образовательного процесса

Руководителями практики (по профилю специальности) от техникума являются преподаватели дисциплин профессионального цикла.

КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Контроль работы практики и отчетность

Общее руководство преддипломной практикой студентов со стороны техникума осуществляет заместитель директора по учебно-производственной работе. Текущий контроль над преддипломной практикой студентов осуществляется руководителем практики от учебного заведения и руководителем практики от организации. В задачи текущего контроля входит контроль посещения баз практики, полноты и качества формирования накопительной папки обучающихся.

Результаты преддипломной практики оцениваются на основании представленной студентом отчетной документации и учитываются при прохождении государственной итоговой аттестации.

Оценка результатов освоения производственной (преддипломной) практики

Аттестация обучающихся по итогам преддипломной практики проводится на основании представленной обучающимся отчетной документации: дневника практики, отчета, характеристики, аттестационного листа в соответствии с заданием на практику.

По результатам практики руководителями практики от организации и от техникума формируется аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций, а также характеристика на обучающегося по освоению общих компетенций в период прохождения практики.

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 в соответствии с заданием на практику.

Студенты, не прошедшие практику или получившие отрицательную оценку не допускаются к прохождению государственной итоговой аттестации.