Министерство образования, науки и молодежной политики
Краснодарского края
Государственное бюджетное профессиональное образовательное учреждение
Краснодарского края «Пашковский сельскохозяйственный колледж»

Рассмотрена на заседании
методического объединения
информационных технологий
Протокол № 1
от «28» сент. 2022г.
Н.Я. Бурмакина

Рассмотрена на заседании
педагогического совета
Протокол № 2
от «26» 10 2022г.

СОГЛАСОВАНО
Зам. директора по
производственному обучению
Орехова Т.В.
«26» 10 2022г.

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

По специальности:

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Краснодар, 2022

Входит в структуру основной образовательной программы, предназначена для ее реализации в соответствии с требованиями ФГОС среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, (Приказ Министерства образования и науки РФ от 09 декабря 2016 г. №1553 (ред. 17.12.2020)), зарегистрирован в Минюсте России от 26.12.2016 №44938 и профессиональным стандартом 16199 «Оператор электронно-вычислительных машин».

Организация разработчик: ГБПОУ КК ПСХК

Разработчик:

Глухова С.В., преподаватель компьютерных дисциплин ГБПОУ КК ПСХК, высшей квалификационной категории, физик, преподаватель, преподавание информатики в общеобразовательных учреждениях

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

1.1. Место производственной практики в структуре основной профессиональной образовательной программы (далее - ООП)

Программа производственной практики является частью ООП по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основных видов профессиональной деятельности:

– эксплуатация автоматизированных (информационных) систем в защищённом исполнении;

– защита информации в автоматизированных системах программными и программно-аппаратными средствами;

– защита информации техническими средствами;

– выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

1.2. Цели и задачи производственной практики

Производственная практика направлена на совершенствование практического опыта обучающихся, развитие общих и профессиональных компетенций, проверку их готовности к самостоятельной трудовой деятельности в условиях реального производства на базе конкретного предприятия.

Целью производственной практики (по профилю специальности) является закрепление, расширение, углубление и систематизация знаний, умений и навыков, полученных при изучении дисциплин профессионального цикла, на основе изучения деятельности конкретной организации, приобретение первоначального практического опыта.

Задачами производственной практики (по профилю специальности) являются:

– закрепление и расширение теоретических и практических знаний;

– развитие профессиональных навыков и навыков деловой коммуникации;

– изучение информационной структуры предприятия, как объекта информатизации;

– сбор необходимых материалов для написания отчета по практике;

– проведение анализа и обобщения результатов собственных исследований.

Производственная практика (преддипломная) направлена на углубление первоначального практического опыта обучающихся, развитие общих и профессиональных компетенций, проверку их готовности к самостоятельной трудовой деятельности, а также на подготовку к выполнению выпускной квалификационной работы в организациях различных организационно-правовых форм.

Целью производственной практики (преддипломной) является подготовка обучающихся к государственной итоговой аттестации, закрепление, расширение, углубление и систематизация знаний, умений и навыков, полученных при изучении дисциплин профессионального цикла, на основе изучения деятельности конкретной организации, приобретение первоначального практического опыта, а также сбор, систематизация и обобщение практического материала, в т.ч. для использования в выпускной квалификационной работе.

Задачами производственной практики (преддипломной) являются:

– закрепление и расширение теоретических и практических знаний;

– развитие профессиональных навыков и навыков деловой коммуникации;

– изучение информационной структуры предприятия, как объекта информатизации;

– сбор необходимых материалов для написания отчета по практике;

– сбор практикантами материалов для выполнения выпускной квалификационной работы и подготовки к государственной итоговой аттестации, закрепление и углубление в производственных условиях знаний и умений, полученных обучающимися при изучении общих профессиональных дисциплин и во время прохождения практики по профилю специальности на основе изучения деятельности конкретного предприятия;

– ознакомление непосредственно на производстве с передовой технологией, организацией труда и экономикой производства;

– развитие профессионального мышления и организаторских способностей в условиях трудового коллектива;

– проведение анализа и обобщения результатов собственных исследований.

С целью овладения указанными видами профессиональной деятельности студент в ходе данного вида практики должен:

Вид профессиональной деятельности: эксплуатация автоматизированных (информационных) систем в защищённом исполнении

Иметь 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 том 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 защиты информации в компьютерных сетях;*

– *установки средств межсетевого экранирования в соответствии с действующими требованиями по защите информации*

– *инструктажа пользователей по порядку безопасной работы 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.*

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;*

– *выполнять конфигурацию 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-аппаратные средства защиты информации в компьютерных сетях;*

– *настраивать и 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 с использованием NAT и скрытого NAT;*

– *определять предложения по применению программных и программно-аппаратных средств защиты информации в компьютерных сетях;*

– *настраивать правила Spanning Tree Protocol в компьютерных сетях;*

– *вносить предложения по применению средств защиты информации в режиме функционирования;*

– *настраивать правила фильтрации пакетов в модели OoS;*

– *управлять количеством подключаемых к портам коммутатора пользователей;*

– *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;*

– *блокировать атаки с помощью межсетевого экрана;*

– *оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях*

Знать:

– состав и принципы работы автоматизированных систем, операционных систем и сред;

– принципы разработки алгоритмов программ, основных приемов программирования;

– модели баз данных;

– принципы построения, физические основы работы периферийных устройств;

– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;

– порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;

– принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;

– *порядок обеспечения безопасности информации при эксплуатации*

– *операционных систем;*

– *типовые средства защиты информации в операционных системах;*

– *встроенный в Microsoft Windows межсетевой экран Брандмауэр Windows;*

– *сканер системы Windows Defender*

– *планирование систем и их приемку;*

– *шифрование сменных носителей информации;*

– *правила политики безопасности «Deny write access to removable drives not protected BitLocker»;*

– *виды политик управления доступом и информационными потоками применительно к операционным системам;*

– *формы и методы инструктажа пользователей по порядку работы в операционных системах;*

– *порядок настройки программного обеспечения систем управления базами данных и средств электронного документооборота;*

– *методы установки ПО рабочих станциях и сервера;*

– *проверку работоспособности системы;*

– *восстановление работоспособности системы;*

– *оптимизацию работоспособности системы;*

– *настройку работоспособности системы управления базами данных;*

– *состав, типовые конфигурации и режимы функционирования программно-аппаратных средств защиты информации;*

– *порядок организации эффективной работы, реализации методов и программных средств межсетевого экранирования;*

– *виды политик управления доступом и информационными потоками в компьютерных сетях;*

– *альтернативные таблицы маршрутизации;*

– *ограничение (шейпинг) трафика.*

Вид профессиональной деятельности: защита информации в автоматизированных системах программными и программно-аппаратными средствами

Иметь 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;

– *определение правил и процедур управления системой защиты информации автоматизированной системы;*

– *определение правил и процедур выявления инцидента;*

– *определение правил и процедур реагирования на инцидент;*

– *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 безопасности информации автоматизированной системы;*

– *проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы.*

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 мониторинги 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;*

– *классифицировать каналы утечки информации;*

– *реализовывать многоуровневую политику разграничения доступа средствами программно-аппаратного комплекса «Страж NT»;*

– *реализовывать защитные механизмы в условно-бесплатное и свободно-распространяемое ПО;*

– *устранять известные уязвимости автоматизированной системы, приводящих к возникновению угроз безопасности информации;*

– *разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированной системы;*

– *обеспечивать безопасность рабочих станций и серверов;*

– *применять режимы работы блочных шифров, схемы кратного шифрования;*

– *проводить криптоанализ алгоритмов с открытым ключом;*

– *подбирать оборудование для реализации проекта беспроводной сети предприятия.*

Знать:

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– основные понятия криптографии и типовых криптографических методов и средств защиты информации;

– особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

– *доктрину информационной безопасности Российской Федерации, № Пр-18954 от 9 сентября 2000г.;*

– *положение о методах и способах защиты информации в информационных системах персональных данных (Утверждено приказом ФСТЭК России от 5 февраля 2010 г. № 58);*

– *руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;*

– *основные методы снижения затрат на защиту информации в автоматизированных системах;*

– *сущностные проявления угрозы;*

– *определение причин и условий дестабилизирующего воздействия на информацию;*

– *методику выявления способов воздействия на информацию;*

– *защиту носителей информации*

– *выбор надежного оборудования;*

– *порядок создания автоматизированных систем в защищенном исполнении. Общие положения. ГОСТ Р-2014 Защита информации;*

– *особенности построения защищенных автоматизированных систем на основе существующих компонентов;*

– *уровни контроля на отсутствие недекларированных возможностей (НДВ) в ПО средств защиты информации;*

– *средства ликвидации последствий от вредоносного ПО;*

– *ответственность за создание, использование и распространение вредоносного ПО;*

– *построение системы антивирусной защиты серверов и рабочих станций;*

– *системы обнаружения и предотвращения вторжений (IDS, IPS);*

– *разработка стратегического плана построения системы защиты;*

– *разработка методов реагирования в случае инцидентов и восстановление;*

– *классификация методов защиты информации от несанкционированного копирования;*

– *альтернативные способы уничтожения данных*

– *бесконтактные смарт-карты и usb-ключи;*

– *направления совершенствования СОВ;*

– *безопасность сетевых устройств OSI;*

– *подготовка и технологии проведения и создания карты покрытия;*

– *реализация технологий брандмауэра;*

– *линейка оборудования для беспроводных сетей;*

– *особенности обеспечения безопасности в беспроводных локальных сетях;*

– *сервисы безопасности VPN;*

– *классификация VPN по рабочему уровню модели OSI;*

– *классификация VPN по архитектуре технического решения;*

– *VPN-решения для построения защищенных корпоративных сетей;*

– *технические и экономические преимущества внедрения технологий VPN в корпоративные сети;*

– *технические и экономические преимущества внедрения технологий VPN в корпоративные сети;*

– *обзор современных межсетевых экранов;*

– *проблемы в сфере сертификации межсетевых экранов;*

– *применение механизмов и служб защиты;*

– *основные этапы создания СМИБ;*

– *система централизованного управления событиями информационной безопасности;*

– *система для децентрализованного управления безопасностью, событиями и информацией;*

– *система выявления угроз в режиме онлайн;*

– *меры защиты информации в государственных информационных системах;*

– *содержание мер защиты информации в информационной системе;*

– *комплексные средства обеспечения защиты рабочих станций и серверов на уровне данных, приложений, сети, ОС и периферийного оборудования;*

– *отечественные типовые решения для построения VPN;*

– *современная антивирусная индустрия: отечественные и зарубежные разработки;*

– *правовые основы обеспечения антивирусной защиты информационных систем;*

– *организация антивирусной защиты на предприятии;*

– *DLP системы: назначение и принципы работы;*

– *применение современных программных и аппаратных криптографических средств для организации защищенных компьютерных систем;*

– *оценка защищенности систем электронных платежей.*

Вид профессиональной деятельности: защита информации техническими средствами

Иметь 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 средств 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;*

– *использования основных методов и средств обеспечения информационной безопасности компьютерных средств;*

– *применения методов криптографической защиты и аутентификации.*

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 помещения от утечки информации по виброакустическому каналу;*

– *проводить статистический анализ загрузки заданного диапазона и обнаружения радиозакладных устройств в защищаемом помещении;*

– *проводить техническое обслуживание и устранять выявленные неисправности технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок;*

– *оценивать защищенность телефонных каналов;*

– *оценивать защищенность помещения от утечки информации по каналам акустоэлектрических преобразований технических средств;*

– *обнаруживать ПЭМИ по электрической составляющей электромагнитного поля;*

– *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 защищенности объекта информатизации;*

– *разрабатывать проект системы видеонаблюдения для организации;*

– *проводить оценку разведдоступности;*

– *проводить комплекс работ по проверке возможности утечки информации по техническим каналам;*

– *проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации;*

– *выполнять правила эксплуатации средств защиты информации*

– *ставить цели, формулировать задачи, связанные с обеспечением корпоративной защиты от внутренних угроз информационной безопасности;*

– *анализировать тенденции развития систем обеспечения корпоративной защиты от внутренних угроз информационной безопасности;*

– *осуществлять установку, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз;*

– *применять знания о корпоративной защите от внутренних угроз информационной безопасности в решении поставленных задач;*

– *осуществлять разработку политик безопасности в системе*

– *корпоративной защиты информации от внутренних угроз;*

– *классифицировать информацию с ограниченным доступом применительно к видам тайны;*

– *грамотно применять методы криптографической защиты;*

– *применять системы управления средствами безопасности;*

– *проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;*

– *администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;*

– *осуществлять установку и конфигурирование систем VPN;*

– *создавать (обновлять) узлы, пользователей, ключи, сертификаты для обеспечения работоспособности защищенной связи с использованием VPN-системы.*

Знать:

– порядок технического обслуживания технических средств защиты информации;

– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

– физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и

– методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

– порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

– номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

– основные принципы действия и характеристики технических средств физической защиты;

– основные способы физической защиты объектов информатизации;

– номенклатуру применяемых средств физической защиты объектов информатизации;

– *технические каналы утечки информации при передаче ее по каналам связи;*

– *демаскирующие признаки объектов;*

– *средства выявления каналов утечки информации;*

– *возможности технической разведки, формы разведывательной деятельности;*

– *основные этапы и процедуры добывания информации технической разведкой;*

– *нормативные документы по противодействию технической разведке;*

– *возможности средств акустической речевой разведки;*

– *особенности реализации пассивных мер защиты в виброакустических каналах утечки речевой информации;*

– *средства контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок;*

– *порядок устранения неисправностей средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок;*

– *организацию ремонта средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок;*

– *возможности приборов видеонаблюдения;*

– *защиту информации в оптическом диапазоне частот;*

– *средства оценки и анализа оптического канала утечки информации;*

– *способы уничтожения информации;*

– *специальные средства для экспресс-копирования (или ее уничтожения) с магнитных носителей;*

– *специальные технические средства для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи;*

– *нормативные документы, регламентирующие применения технических средств защиты информации;*

– *скрытие и защита информации по техническим каналам;*

– *методы и средства инженерной защиты и технической охраны объектов;*

– *порядок эксплуатации программных и технических средств и систем защиты секретной информации от НСД;*

– *порядок приемки СЗСИ перед сдачей в эксплуатацию в составе АС;*

– *типовой вариант КПП;*

– *быстроразвертываемые комплексы ТСО, их состав, особенности, преимущества от внедрения;*

– *номенклатуру применяемых средств обнаружения (вибрационные, комбинированные, магнитеметрические, объектовые);*

– *сравнительный анализ применения шлюзового турникета и маятниковой двери-шлюза;*

– *организацию охраны объектов с применением технических средств воздействия;*

– *нормативную документацию использования технических средств физической защиты;*

– *единую систему конструкторской документации;*

– *единую систему технологической документации;*

– *особенности выбора инженерно-технических средств физической защиты периметров протяженных объектов, особенности их монтажа;*

– *объекты компьютерных технологий, используемые в обеспечении корпоративной защиты от внутренних угроз информационной безопасности;*

– *понятийный аппарат информационных технологий и особенности терминологии в области корпоративной защиты от внутренних угроз информационной безопасности;*

– *базовые составляющие в области развития систем информационной безопасности;*

– *методы выявления утечек информации с использованием технологии Data Leakage Prevention (DLP);*

– *методы проведения анализа в области обеспечения корпоративной защиты от внутренних угроз информационной безопасности;*

– *современные технологии, применяемых в области корпоративной защиты от внутренних угроз информационной безопасности;*

– *функционирование системы управления средствами безопасности;*

– *основные типы моделей управления доступом;*

– *обследование (аудит) организации с целью защиты от угроз информационной безопасности;*

– *методы защиты сетевого трафика с использованием VPN-технологий.*

Вид профессиональной деятельности: выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

Иметь 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.*

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 антивирусных программ;*

– *осуществлять резервное копирование и восстановление данных.*

Знать:

– *требования техники безопасности при работе с вычислительной техникой;*

– *основные принципы устройства и работы компьютерных систем и периферийных устройств;*

– *классификацию и назначение компьютерных сетей;*

– *виды носителей информации;*

– *программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета;*

– *основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.*

1.3. Количество недель (часов) на освоение программы производственной практики:

Всего 16 недель, 576 часов, в том числе:
на производственную практику (по профилю специальности) ПП.01 - 2 недели, 72 часа;
на производственную практику (по профилю специальности) ПП.02 - 2 недели, 72 часа;
на производственную практику (по профилю специальности) ПП.03 - 6 недель, 216 часов;
на производственную практику (по профилю специальности) ПП.04 - 2 недели, 72 часа;
на производственную практику (преддипломную) ППП - 4 недели, 144 часа.

2. РЕЗУЛЬТАТЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Результатом производственной практики является освоение:
общих компетенций (ОК):

Код	Наименование результата практики
ОК1. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; – адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач
ОК2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	– использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач
ОК3. Планировать и реализовывать собственное профессиональное и личностное развитие	– демонстрация ответственности за принятые решения – обоснованность самоанализа и коррекция результатов собственной работы;
ОК4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	– взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; – обоснованность анализа работы членов команды (подчиненных)
ОК5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	– грамотность устной и письменной речи, – ясность формулирования и изложения мыслей
ОК6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей	– соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,
ОК7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	– эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; – знание и использование ресурсосберегающих технологий в области телекоммуникаций

ОК8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	– эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;
ОК9. Использовать информационные технологии в профессиональной деятельности	– эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;
ОК10. Пользоваться профессиональной документацией на государственном и иностранном языках	– эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.

профессиональных компетенций (ПК):

Вид профессиональной деятельности	Код	Наименование результатов практики
Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Демонстрирует умения установки и настройки 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	Проявляет умения и практический опыт администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении
	ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с	Проводит перечень работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

	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	Проявляет знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК 2.1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрирует умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации
	ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно- аппаратными средствами.	Демонстрирует знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
	ПК 2.3 Осуществлять тестирование функций отдельных программных и программно- аппаратных средств защиты информации.	Выполняет перечень работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации
	ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявляет знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа
	ПК 2.5 Уничтожать информацию и носители информации с использованием программных и программно- аппаратных средств.	Демонстрирует алгоритм проведения работ по уничтожению информации и носителей 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.	Проявляет знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
Защита информации техническими средствами	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрирует умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания 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.	Проявляет умения и практический опыт в эксплуатации 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.	Проводит работы по измерению 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	Проводит самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых

	техническими средствами защиты информации.	техническими средствами защиты информации
	ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Проявляет знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации
	ПК 3.6. *Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах*	*Проводит работы с защищенными автоматизированными системами. Передает информацию по защищенным каналам связи*
	ПК 3.7. *Выявлять и анализировать возможные угрозы информационной безопасности объектов*	*Проявляет умения и практический опыт выявления возможных угроз информационной*
	ПК 3.8. *Ориентироваться в условиях частой смены технологий в профессиональной деятельности*	*Имеет практический опыт выявления возможных угроз информационной безопасности объектов защиты*
	ПК 3.9. *Проводить регламентные работы и фиксировать отказы средств защиты*	*Фиксирует отказы в работе средств вычислительной техники*
Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	*ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения*	*Демонстрирует умения и практические навыки в подготовке оборудования компьютерной системы к работе, производит 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	*Проявляет умения и практический опыт в работе с текстовыми документами, таблицами и презентациями, а также базами данных*

	ПК 4.3. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	*Умеет пользоваться ресурсами локальных вычислительных сетей, осуществлет поиск, анализ и интерпретацию информации*
	ПК 4.4. Обеспечивать применение средств защиты информации в компьютерной системе	*Применяет средства защиты информации в компьютерной системе*
Преддипломная практика	ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Демонстрирует умения установки и настройки 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	Проявляет умения и практический опыт администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении
	ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Проводит перечень работ по обеспечению бесперебойной работы 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	Проявляет знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных

	в защищенном исполнении	(информационных) систем в защищенном исполнении
	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрирует умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации
	ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно- аппаратными средствами.	Демонстрирует знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
	ПК 2.3 Осуществлять тестирование функций отдельных программных и программно- аппаратных средств защиты информации.	Выполняет перечень работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации
	ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявляет знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа
	ПК 2.5 Уничтожать информацию и носители информации с использованием программных и программно- аппаратных средств.	Демонстрирует алгоритм проведения работ по уничтожению информации и носителей 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.	Проявляет знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрирует умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания 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.	Проявляет умения и практический опыт в эксплуатации 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.	Проводит работы по измерению 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.	Проводит самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
	ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Проявляет знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации
	ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание	*Демонстрирует умения и практические навыки в подготовке оборудования компьютерной системы к работе, производит инсталляцию, настройку и*

	программного обеспечения	*обслуживание программного обеспечения*
	ПК 4.2. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах	*Проявляет умения и практический опыт в работе с текстовыми документами, таблицами и презентациями, а также базами данных*
	ПК 4.3. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	*Умеет пользоваться ресурсами локальных вычислительных сетей, осуществляет поиск, анализ и интерпретацию информации*
	ПК 4.4. Обеспечивать применение средств защиты информации в компьютерной системе	*Применяет средства защиты информации в компьютерной системе*

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Тематический план

Коды формируемых компетенций	Наименование профессионального модуля	Объем времени, отведенный на практику (в неделях, часах)	Сроки проведения
ПК 1.1 – ПК 1.4	Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	2 недели, 72 часа	По графику учебного процесса
ПК 2.1 – ПК 2.6	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	2 недели, 72 часа	По графику учебного процесса
ПК 3.1 – ПК 3.5 *ПК 3.6 – ПК 3.9*	Защита информации техническими средствами	6 недель, 216 часов	По графику учебного процесса
ПК 4.1 – ПК 4.4	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	2 недели, 72 часа	По графику учебного процесса
ПК 1.1 – 1.4 ПК 2.1 – 2.6 ПК 3.1 – 3.5 ПК 4.1 – 4.4	Преддипломная практика	4 недели, 144 часа	По графику учебного процесса

3.2. Содержание практики ПМ 01

Виды деятельности	Виды работ	Содержание освоенного учебного материала, необходимого для выполнения видов работ	Наименование учебных дисциплин, междисциплинарных курсов с указаниями тем, обеспечивающих выполнение видов работ	Количество часов (недель)
Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	Ознакомление с организацией (предприятием) – базой прохождения практики	Проведение вводного инструктажа по правилам внутреннего трудового распорядка предприятия, инструктажа по технике безопасности и пожарной безопасности. Знакомство с предприятием, режимом его работы, с правилами внутреннего распорядка, рабочим местом и руководителем практики от предприятия (организации). Знакомство с организационной структурой организации (предприятия), видами деятельности. Изучение деятельности структурного подразделения, функций, задач, структуры, в котором проходит практика. Изучение технической документации ПЭВМ и периферийных устройств, имеющихся на данном предприятии. Технические характеристики ПК, предоставленного обучающемуся для	МДК.01.01. Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем Тема 1.3. Модульная структура операционных систем, пространство пользователя Тема 1.5. Управление процессами, многопроцессорные системы Тема 1.6. Виртуализация и облачные технологии Тема 2.1. Принципы построения защиты информации в операционных системах	6

		выполнения заданий на время прохождения производственной практики.	Тема 3.3. Серверные операционные системы МДК.01.02 Тема 1.3. Базовые понятия и классификация систем управления базами данных Тема 4.1. Структурированный язык запросов SQL Тема 4.2. Операторы и функции языка SQL Тема 5.3. Клиентская часть распределенной базы данных Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных Тема 6.2. Перехват исключительных ситуаций и обработка ошибок Тема 6.3. Механизмы защиты информации в системах управления базами данных	
	Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.		6
	Обслуживание средств защиты информации прикладного и системного программного обеспечения.	Участие в обслуживании средств защиты информации прикладного и системного программного обеспечения.		6
	Настройка программного обеспечения с соблюдением требований по защите информации.	Настройка программного обеспечения с соблюдением требований по защите информации.		6
	Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам.	Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам.		6
	Настройка встроенных средств защиты	Настройка встроенных средств защиты информации программного обеспечения.		6

	информации программного обеспечения. Проверка функционирования встроенных средств защиты информации программного обеспечения.	Проверка функционирования встроенных средств защиты информации программного обеспечения.	МДК.01.03. Тема 1.3. Типовые каналы передачи и их характеристики Тема 2.2. Беспроводные системы передачи данных Тема 2.3. Сотовые и спутниковые системы	
	Своевременное обнаружение признаков наличия вредоносного программного обеспечения.	Своевременное обнаружение признаков наличия вредоносного программного обеспечения.	МДК.01.04 Тема 1.3. Угрозы безопасности информации в автоматизированных системах Тема 1.4. Основные меры защиты информации в автоматизированных системах Тема 1.6. Защита информации в распределенных автоматизированных системах Тема 1.7. Особенности разработки информационных систем персональных данных	6
	Обслуживание средств защиты информации в компьютерных системах и сетях. Обслуживание систем защиты информации в автоматизированных системах.	Участие в обслуживании средств защиты информации в компьютерных системах и сетях. Участие в обслуживании систем защиты информации в автоматизированных системах.		6
	Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем. Проверка работоспособности системы защиты	Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем. Участие в проверке работоспособности системы защиты информации автоматизированной системы.		6

	информации автоматизированной системы.		Тема 2.2. Администрирование автоматизированных систем Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении Тема 2.4. Защита от несанкционированного доступа к информации Тема 2.7. Документация на защищаемую автоматизированную систему МДК.01.05. Тема 2.2. Начальная настройка коммутатора Тема 2.3. Виртуальные локальные сети (VLAN) Тема 2.4. Функции повышения надежности и производительности Тема 2.7. Функции обеспечения безопасности и	
	Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации. Контроль стабильности характеристик системы защиты информации автоматизированной системы.	Проверка соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации. Проверка стабильности характеристик системы защиты информации автоматизированной системы.		6
	Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем.	Участие в ведении технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем.		6
	Инструктаж пользователей о соблюдении требований по защите информации	Проведение инструктажа для пользователей о соблюдении требований по защите информации при работе с программным обеспечением.		4

	при работе с программным обеспечением. Подготовка отчетной документации.	Систематизация и анализ выполненных заданий, оформление отчетной документации.	ограничения доступа к сети Тема 3.1. Основные принципы создания надежной и безопасной. ИТ-инфраструктуры Тема 3.3. Системы обнаружения и предотвращения проникновений.	
Промежуточная аттестация в форме дифференцированного зачета				2
Всего				**72 (2 недели)**

Содержание практики ПМ 02

Виды деятельности	**Виды работ**	**Содержание освоенного учебного материала, необходимого для выполнения видов работ**	**Наименование учебных дисциплин, междисциплинарных курсов с указаниями тем, обеспечивающих выполнение видов работ**	**Количество часов (недель)**
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Ознакомление с организацией (предприятием) – базой прохождения практики	Проведение вводного инструктажа по правилам внутреннего трудового распорядка предприятия, инструктажа по технике безопасности и пожарной безопасности. Знакомство с предприятием, режимом его работы, с правилами внутреннего распорядка, рабочим местом и	МДК 02.01 Тема 1.2. Стандарты безопасности Тема 1.3. Защищенная автоматизированная система	6

		руководителем практики от предприятия (организации). Знакомство с организационной структурой организации (предприятия), видами деятельности. Изучение деятельности структурного подразделения, функций, задач, структуры, в котором проходит практика. Сбор информации о видах обеспечения автоматизированных систем предприятия (организации). Изучение технической документации ПЭВМ и периферийных устройств, имеющихся на данном предприятии. Технические характеристики ПК, предоставленного обучающемуся для выполнения заданий на время прохождения производственной практики.	Тема 1.4. Дестабилизирующее воздействие на объекты защиты Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа Тема 2.1. Основы защиты автономных автоматизированных систем Тема 2.4. Защита программ и данных от несанкционированного копирования Тема 2.5. Защита информации на машинных носителях Тема 2.7. Системы обнаружения атак и вторжений Тема 3.1. Основы построения защищенных сетей Тема 3.2.	
	Анализ принципов построения систем информационной защиты производственных подразделений.	Выявление принципов построения систем информационной защиты производственных подразделений. Анализ принципов построения систем информационной защиты производственных подразделений		6
	Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.	Определение состава элементов программной и аппаратной защиты автоматизированной системы. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.		6

		Документирование эксплуатации системы защиты автоматизированной системы.	Средства организации VPN	
	Участие в диагностировании программно-аппаратных средств обеспечения информационной безопасности.	Участие в диагностировании программно-аппаратных средств обеспечения информационной безопасности.	Тема 4.1. Обеспечение безопасности межсетевого взаимодействия Тема 6.1.	6
	Участие в устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности.	Участие в устранении отказов программно-аппаратных средств обеспечения информационной безопасности. Участие в обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности.	Мониторинг систем защиты Тема 6.2. Изучение мер защиты информации в информационных системах МДК 02.02. Тема 3.4. Аутентификация данных. Электронная подпись Тема 3.6. Криптозащита информации в сетях передачи данных	6
	Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении.	Определение состава программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении.		6

	Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	Участие в обеспечении учета и обработки, конфиденциальной информации. Участие в процессах хранения и передачи конфиденциальной информации.		6
	Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	Применение нормативных правовых актов, по обеспечению информационной безопасности программно- аппаратными средствами при работе в структурном подразделении. Применение нормативных методических документов по обеспечению информационной безопасности программно- аппаратными средствами при выполнении задач практики		6
	Определение правил и процедур управления системой защиты информации автоматизированной системы. Выявления и реагирования на инцидент.	*Определение правил управления системой защиты информации автоматизированной системы.* *Определение процедур управления системой защиты информации автоматизированной системы.* *Определение правил выявления и реагирования на инцидент.* *Определение процедур выявления и реагирования на инцидент.*		6
	Выбор и обоснование критериев выбора эффективности функционирования защищенных	*Выбор и обоснование критериев выбора эффективности функционирования защищенных автоматизированных систем.*		6

	автоматизированных систем.	*Оценка эффективности функционирования защищенных автоматизированных систем.*		
	Проведение экспертизы состояния защищенности информации автоматизированных систем. Уточнение модели угроз безопасности информации автоматизированной системы	*Проведение экспертизы состояния защищенности информации автоматизированных систем.* *Документирование результатов экспертизы.* *Уточнение модели угроз безопасности информации автоматизированной системы.* *Разработка раздела политики информационной безопасности.*		6
	Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы. Подготовка отчетной документации	*Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы.* *Проведение практических занятий с персоналом в тестовой зоне.* *Отработка ситуационных задач.* Систематизация и анализ выполненных заданий, оформление отчетной документации.		4
Промежуточная аттестация в форме дифференцированного зачета				2
Всего				**72** **(2 недели)**

Содержание практики ПМ 03

Виды деятельности	Виды работ	Содержание освоенного учебного материала, необходимого для выполнения видов работ	Наименование учебных дисциплин, междисциплинарных курсов с указаниями тем, обеспечивающих выполнение видов работ	Количество часов (недель)
Защита информации техническими средствами	Ознакомление с организацией (предприятием) – базой прохождения практики	Проведение вводного инструктажа по правилам внутреннего трудового распорядка предприятия, инструктажа по технике безопасности и пожарной безопасности. Знакомство с предприятием, режимом его работы, с правилами внутреннего распорядка, рабочим местом и руководителем практики от предприятия (организации). Знакомство с организационной структурой организации (предприятия), видами деятельности. Изучение деятельности структурного подразделения, функций, задач, структуры, в котором проходит практика. Изучение технической документации ПЭВМ и периферийных устройств, имеющихся на данном предприятии. Технические характеристики ПК, предоставленного обучающемуся для	МДК.03.01 Тема 2.2. Технические каналы утечки информации Тема 2.3. Методы и средства технической разведки Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок Тема 4.1. Системы защиты от утечки информации по акустическому каналу Тема 4.2. Системы защиты от утечки информации по проводному каналу	6

		выполнения заданий на время прохождения производственной практики.	Тема 4.3. Системы защиты от утечки информации по вибрационному каналу Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу Тема 4.5. Системы защиты от утечки информации по телефонному каналу Тема 4.6. Системы защиты от утечки информации по электросетевому каналу Тема 4.7. Системы защиты от утечки информации по оптическому каналу Тема 5.1. Применение технических средств защиты информации Тема 5.2. Эксплуатация технических средств защиты информации МДК.03.02 Тема 2.1 Система обнаружения комплекса	
	Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации.	Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации		6
	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 охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.		6
	Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам.	Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам		6
	Техническое обслуживание средств защиты информации.	*Обслуживание средств защиты информации.*		6
	Участие в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет	*Участие в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты*		6

	соответствия требованиям защиты информации по соответствующим классам безопасности.	*информации по соответствующим классам безопасности.*	инженерно-технических средств физической защиты Тема 2.2. Система контроля и управления доступом Тема 2.3. Система телевизионного наблюдения Тема 2.4. Система сбора, обработки, отображения и документирования информации Тема 3.1 Применение инженерно-технических средств физической защиты Тема 3.2. Эксплуатация инженерно-технических средств физической защиты МДК 03.03 *Тема 1.2. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз*	
	Проведение контрольных проверок работоспособности и эффективности действующих систем и технических средств защиты информации, составление и оформление акты контрольных проверок.	*Участие в проведении контрольных проверок работоспособности и эффективности действующих систем и технических средств защиты информации, составление и оформление акты контрольных проверок.*		6
	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами	Ознакомление и применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами		6
	Участия в мониторинге эффективности технических средств защиты информации.			6
	Диагностика, устранение отказов и неисправностей, восстановление работоспособности	Диагностика технических средств защиты информации, устранение отказов и неисправностей, восстановление их работоспособности.		6

	технических средств защиты информации.		*Тема 1.3. Исследование (аудит) организации с целью защиты от внутренних угроз* *Тема 1.4. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз* *Тема 1.5. Технологии агентского мониторинга* *Тема 2.2. Базовый программный комплекс VipNet Administrator* *Тема 2.4. Центр управления политиками безопасности ViPNet Policy Manager* *Тема 2.6. Программно-аппаратный комплекс (ПАК) Координатор VipNet HW4*	
	Проведение 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.	Проведение 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.		6
	Проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.		6
	Установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических	Установка, монтаж и настройка инженерно-технических средств физической защиты. Техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности.		6

	средств физической защиты.			
	Применение технических средств для криптографической защиты информации конфиденциального характера.	Применение технических средств для криптографической защиты информации конфиденциального характера.		6
	Применение технических средств для уничтожения информации и носителей информации.	Применение технических средств для уничтожения информации и носителей информации.		6
	Оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу.	*Проведение оценки защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу.*		6
	Проведение статистического анализа загрузки заданного диапазона и обнаружения радиозакладных устройств в защищаемом помещении.	*Проведение статистического анализа загрузки заданного диапазона и обнаружения радиозакладных устройств в защищаемом помещении.*		6
	Проведение технического обслуживания и устранение выявленных неисправностей технических средств защиты информации от	*Проведение технического обслуживания и устранение выявленных неисправностей технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.*		6

	утечки за счет побочных электромагнитных излучений и наводок.			
	Оценка защищенности телефонных каналов. Оценка защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств.	*Проведение оценки защищенности телефонных каналов. Защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств.*		6
	Проведение испытания защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами.	*Ознакомление с инструкциями по эксплуатации и эксплуатационно-техническими документами. Проведение испытания защищенных технических средств обработки информации в соответствии с инструкциями.*		6
	Организация технического контроля эффективности мер защиты информации.	*Организация технического контроля эффективности мер защиты информации.*		6
	Разработка проекта системы видеонаблюдения для организации.	*Разработка проекта системы видеонаблюдения для организации.*		6
	Изучение структуры организации на основании полученных материалов	*Изучение структуры организации, проведение обследования корпоративных информационных систем.*		6

	(«модели организации»), проведение обследования корпоративных информационных систем.			
	Определение объектов защиты предприятия.	*Определение объектов защиты предприятия.*		6
	Разработка перечня субъектов/персон, роли пользователей, прав доступа в корпоративные информационные системы организации.	*Разработка перечня субъектов/персон, роли пользователей, прав доступа в корпоративные информационные системы организации.*		6
	Определение каналов передачи данных и потенциальных утечек информации в корпоративной информационной системе. Определение типов циркулирующих данных в корпоративной информационной системе.	*Определение каналов передачи данных и потенциальных утечек информации в корпоративной информационной системе. Определение типов циркулирующих данных в корпоративной информационной системе.*		6
	Выявление потоков передачи данных и возможные каналы утечки информации в корпоративной информационной системе.	*Выявление потоков передачи данных и возможные каналы утечки информации в корпоративной информационной системе.*		6

	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз.	*Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз.*		6
	Разработка новых и/или модификация существующих политик безопасности, перекрывающие каналы передачи данных и возможные инциденты.	*Разработка новых и/или модификация существующих политик безопасности, перекрывающие каналы передачи данных и возможные инциденты.*		6
	Использование различных технологий защиты: печатей, бланков, графических объектов, баз данных и т.п.	*Использование различных технологий защиты: печатей, бланков, графических объектов, баз данных и т.п.*		6
	Применение политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизирование числа выявленных инцидентов безопасности.	*Применение политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизирование числа выявленных инцидентов безопасности.*		6
	Заполнение шаблона модели угроз.	*Разработка и заполнение шаблона модели угроз.*		6

	Подготовка отчёта о результатах аудита, включая потоки данных, потенциальные каналы утечек, уровни рисков роли пользователей, объекты защиты (с привязкой к нормативной базе и методикам оценки последствий), ролями пользователей и т.п.	*Подготовка отчёта о результатах аудита, включая потоки данных, потенциальные каналы утечек, уровни рисков роли пользователей, объекты защиты (с привязкой к нормативной базе и методикам оценки последствий), ролями пользователей и т.п.*		6
	Определить перечень нормативных актов РФ, задействованных в рамках модели угроз.	*Определить перечень нормативных актов РФ, задействованных в рамках модели угроз.*		6
	Разработка перечня, описание и шаблонов нормативно правовых документов организации по легальному применению корпоративной защиты от внутренних угроз информационной безопасности.	*Разработка перечня, описание и шаблонов нормативно правовых документов организации по легальному применению корпоративной защиты от внутренних угроз информационной безопасности.*		6
	Подготовка отчетной документации	Систематизация и анализ выполненных заданий, оформление отчетной документации.		4
Промежуточная аттестация в форме дифференцированного зачета				2
Всего				**216 (6 недель)**

Содержание практики ПМ 04

Виды деятельности	Виды работ	Содержание освоенного учебного материала, необходимого для выполнения видов работ	Наименование учебных дисциплин, междисциплинарных курсов с указаниями тем, обеспечивающих выполнение видов работ	Количество часов (недель)
Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	*Ознакомление с организацией (предприятием) – базой прохождения практики*	*Проведение вводного инструктажа по правилам внутреннего трудового распорядка предприятия, инструктажа по технике безопасности и пожарной безопасности.* *Знакомство с предприятием, режимом его работы, с правилами внутреннего распорядка, рабочим местом и руководителем практики от предприятия (организации).* *Знакомство с организационной структурой организации (предприятия), видами деятельности.* *Изучение деятельности структурного подразделения, функций, задач, структуры, в котором проходит практика.* *Изучение технической документации ПЭВМ и периферийных устройств, имеющихся на данном предприятии. Технические характеристики ПК, предоставленного обучающемуся для*	МДК 04.01. Тема 1.1. *Устройства компьютерной системы* Тема 1.2. *Операционная система* Тема 1.3. *Сервисное программное обеспечение и защита информации* Тема 2.1. *Технология обработки текстовой информации* Тема 2.2. *Технология обработки числовой информации* Тема 2.3. *Технология работы с базами данных* Тема 2.4. *Технология работы с*	6

		выполнения заданий на время прохождения производственной практики.	*мультимедийными презентациями*	
	Выполнять настройку интерфейса операционных систем. Управлять файлами данных на локальных, съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в Интернете.	*Выполнение настройки интерфейса операционной системы. Управление файлами данных на локальных, съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в Интернете.*	Тема 3.1. *Ресурсы сетевых технологий и сервисов компьютерных сетей*	6
	Подключать периферийные устройства и компьютерную оргтехнику к персональному компьютеру и настраивать режимы ее работы. *Производить распечатку, копирование и тиражирование документов на принтере и другие периферийные устройства вывода.*	*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.*		6
	Осуществлять резервное копирование и восстановление данных. Диагностировать	*Осуществление резервного копирования и восстановление данных;* *Диагностирование простейших неисправностей персонального*		6

	простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники.	*компьютера, периферийного оборудования и компьютерной оргтехники.*		
	Создавать и управлять содержимым документов с помощью редактора документов.	*Создание и управление содержимым документов с помощью редактора документов.*		6
	Создавать и управлять содержимым таблиц с помощью редакторов таблиц.	*Создание и управление содержимым таблиц с помощью редактора таблиц.*		6
	Создавать и управлять содержимым презентаций с помощью редакторов презентаций.	*Создание и управление содержимым презентаций с помощью редактора презентаций.*		6
	Обрабатывать графическую информацию средствами графических программ.	*Обработка графической информации средствами графических программ.*		6
	Создавать и обмениваться письмами электронной почты. Осуществлять поиск, сортировку и анализ информации с помощью	*Создание и обмен письмами электронной почты; Осуществление поиска, сортировки и анализа информации с помощью поисковых интернет-сайтов.*		6

	поисковых интернет-сайтов.			
	Распознавать сканированные текстовые документы с помощью программ распознавания текста. *Пересылать и публиковать файлы данных в Интернете*	*Распознавание сканированных текстовых документов с помощью программ распознавания текста.* *Пересылка и публикация файлов данных в Интернете.*		6
	Осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ.	*Осуществление антивирусной защиты персонального компьютера с помощью антивирусных программ.*		6
	Вести отчетную и техническую документацию.	*Готовить отчетную и техническую документацию.* *Систематизация и анализ выполненных заданий производственной практики, оформление отчетной документации.*		4
Промежуточная аттестация в форме дифференцированного зачета				2
Всего				**72** **(2 недели)**

Содержание практики преддипломной

Виды деятельности	Виды работ	Содержание освоенного учебного материала, необходимого для выполнения видов работ	Наименование учебных дисциплин, междисциплинарных курсов с указаниями тем, обеспечивающих выполнение видов работ	Количество часов (недель)
Эксплуатация автоматизированных (информационных) систем в защищённом исполнении». Защита информации в автоматизированных системах программными и программно-аппаратными средствами. Защита информации техническими средствами. Выполнение работ по одной или нескольким профессиям рабочих,	Организационные вопросы оформления на предприятии, установочная лекция, инструктаж по охране труда и технике безопасности, распределение по рабочим местам.	Изучение инструкции по охране труда. Изучение инструкции по технике безопасности и пожаробезопасности, схем аварийных проходов и выходов, пожарного инвентаря. Изучение правил внутреннего распорядка. Изучение правил и норм охраны труда, техники безопасности при работе с вычислительной техникой.	МДК 04.01. Тема 1.1. *Устройства компьютерной системы*: «*Режим работы, охрана труда, техника безопасности и оснащение рабочего места оператора. Функциональные обязанности оператора: роль и назначение. Организация рабочего места и санитарные нормы при работе с ПК.»*	6
	Ознакомление со структурой и характером деятельности предприятия.	Определение статуса, структуры и системы управления функциональных подразделений и служб предприятия. Изучение положения об их деятельности и правовой статус.	ПМ 01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	6

должностям служащих.		Изучение должностных инструкций технических работников среднего звена в соответствии с подразделением предприятия.	ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ 03 Защита информации техническими средствами ПМ 04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	
		Ознакомление с перечнем и строением сети. Определение перечня и назначения оборудования.		6
	Сбор материалов для составления технического задания по теме ВКР.	Определение типовых требований к составу и содержанию технического задания (ТЗ): раздел ТЗ и его содержание.		6
		Определение общей цели ВКР.		6
		Определение состава ВКР и функциональных задач.		6
		Разработка и обоснование требований к ВКР.		6
		Определение этапов ВКР и сроков их выполнения		6
	Формирование требований.	Обследование объекта и подготовительная работа с экспертами.		6
		Обоснование необходимости создания или модификации ИС в защищенном исполнении.		6
		Документирование результатов обследования и обоснования необходимости создания или модификации ИС в защищенном исполнении.		6
		Формирование требований к пользователям ИС		6

		Документирование требований к пользователям ИС		6
	Разработка концепции ИС	Изучение объекта с точки зрения функциональной и организационной структуры.		6
		Изучение объекта с точки зрения организации и содержания документооборота.		6
		Проведение необходимых научно-исследовательских работ		6
		Разработка вариантов концепции ИС		6
		Выбор варианта концепции ИС, удовлетворяющего требованиям пользователей		6
	Техническое задание Часть 1. Разработка и утверждение плана технического задания на создание или модификацию ИС в защищенном исполнении Часть 2 Обоснование предварительных проектных решений по отдельным частям ИС Часть 3 Разработка рабочей документации на внедрение ИС	Детализация разделов плана технического задания на создание или модификацию ИС в защищенном исполнении Утверждение технического задания на создание ИС в защищенном исполнении.		6
		Обоснование предварительных проектных решений по ИС в целом Разработка предварительных проектных решений по отдельным частям ИС в защищенном исполнении. Разработка предварительных проектных решений по ИС в целом		6
		Разработка документации на ИС в целом и на ее отдельные части		6
		Разработка документации по техническому сопровождению ИС в период эксплуатации		6

		Разработка документации по обучению пользователей работе с ИС		
		Формирование справочной интерактивной поддержки ИС. Создание или адаптация Интернет- ресурса поддержки ИС.		6
	Оформление отчета о прохождении преддипломной практики.	Оформление отчета в соответствии с методическими указаниями.		4
Аттестация в форме дифференцированного зачета.				2
Всего				**144 (4 недели)**

Варианты заданий преддипломной практики (тематика выпускных квалификационных работ) составляется в соответствии с выбранными темами выпускных квалификационных работ.

4. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

4.1. Место прохождения производственной практики

Реализация программы производственной 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.

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 фирмы, государственные архивы, кадровые агентства.

Организация как база практики должна:

- соответствовать данной специальности и виду практики;
- иметь сферы деятельности, предусмотренные программой практики;
- располагать квалифицированными кадрами для руководства практикой.

4.2. Требования к документации, необходимой для проведения производственной практики:

Для проведения производственной практики (по профилю специальности) в колледже разработана следующая документация:

- положение о практике;
- программа производственной практики, согласованная с работодателями;
- договор с организацией на организацию и проведение практики;
- приказ о педагогической нагрузке преподавателей;
- приказ о распределении студентов по местам прохождения производственной практики и учебной практики в случае ее прохождения на предприятии;
- график проведения производственной практики;
- дневник-отчет.

4.3. Требования к учебно-методическому обеспечению практики:

Дневник-отчет по каждому виду практик.

4.4. 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 производственной практики: рабочее место должно быть оборудовано компьютерной техникой с программным обеспечением профессионального назначения.

4.5. Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы.

Основные источники:

1. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2005. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности.
2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017. - 175 с.
1. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016. - 248 с.
2. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2014.
3. Зайцев А.П., Мещкряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.
4. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2018. - 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
5. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2017. – 416 с.
3. Киселев С.В. Оператор ЭВМ: учеб. пособие для студ. учреждений сред. проф. образования /. – 7-е изд., исп. – М.: Издательский центр «Академия», 2014.
4. Коньков, К. А. Устройство и функционирование ОС Windows. Практикум к курсу Операционные системы. /Учебное пособие // К.А. Коньков. М.: Бином, Лаборатория знаний Интуит, 2013.
6. Костров Б. В., Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2016.
7. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. - 2-е изд.- М.: Горячая линия-Телеком, 2014.
8. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2018
5. Мельников Д. Информационная безопасность открытых систем. - М.: Форум, 2013.
6. Михеева Е.В. Информационные технологии в профессиональной деятельности. – М.: Издательский центр «Академия», 2021.
7. Михеева Е.В. Практикум по информационным технологиям в профессиональной деятельности. – М.: Издательский центр «Академия», 2021.
8. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.
9. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.
9. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2021. – 336с

10. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2015.
11. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.
12. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2013.
13. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
14. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2013
15. Федотова Е.Л. Информационные технологии в профессиональной деятельности. - М: ФОРУМ, 2021. Режим доступа: http://znanium.com
16. Филимонова Е.В. Информационные технологии в профессиональной деятельности. - М: КноРус,2021. Режим доступа: https://www.book.ru
17. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2019

Дополнительные источники:

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. 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.
11. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
12. 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.
13. 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.
14. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
15. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
16. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
17. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
18. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
19. 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.
20. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
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 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
23. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
24. 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
25. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
26. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
27. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
28. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
29. 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
30. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
31. 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
32. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
33. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
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 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
39. 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.
40. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
41. 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.
42. 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.
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.: программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники; базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.
51. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.
52. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2012. – 224 с.
53. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. - СПб: Питер, 2006 - 703 с.
54. Губенков А.А. Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2009. - 88 с.
55. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы – М.: Бином, 2011. – 1024 с.
56. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бином, 2011. – 704 с.
57. Жмакин А. П. Архитектура ЭВМ: учеб. пособие для вузов / А. П. Жмакин. - 2-е изд., перераб. и доп. - СПб: БХВ-Петербург, 2010. - 352 с.: ил. - (Учебная литература для вузов)
58. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник. -М.: Горячая линия-Телеком, 2008
59. Кофлер М., Linux. Полное руководство – Питер, 2018. – 800 с.
60. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие. -М.: Радио и связь, 2008
61. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие. - 2-е изд., исп.- М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2007. - 531 с.
62. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.
63. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов. - 3-е изд., стер. М.: Горячая линия, 2005.- 147 с.
64. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб. пос. для студентов СПО – М.: Форум, 2019. – 544 с.
65. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высших учеб. заведений / В. В. Платонов. – М.: Академия, 2016. – 240 с.
66. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.:

МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 г
67. Сафонов, В.О. Основы современных операционных систем: учебное пособие. М.: Бином. Лаборатория знаний, 2014. – 583 с.
68. Уваров, С. 500 лучших программ для вашего компьютера (2 CD) / С. Уваров. СПб: Питер, 2009. –·320 с.

Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Информационный портал по безопасности www.SecurityLab.ru.
4. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
5. Сайт Научной электронной библиотеки www.elibrary.ru
6. Справочно-правовая система «Консультант Плюс» www.consultant.ru
7. Справочно-правовая система «Гарант» www.garant.ru
8. Федеральный портал «Российское образование www.edu.ru
9. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
10. Российский биометрический портал www.biometrics.ru
11. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp://www.ict.edu.ru
12. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
13. Федеральный портал «Российское образование» www.edu.ru

4.6. Требования к руководителям практики от образовательного учреждения и организации.

Руководство производственной практикой от колледжа осуществляют преподаватели дисциплин профессионального или междисциплинарного цикла, соответствующих профилю профессиональных модулей. Квалификация педагогических работников образовательной организации должна отвечать квалификационным требованиям, указанным в профессиональном стандарте.

Руководители практики от колледжа:

– перед её началом консультируют обучающихся о выполнении заданий программы практики и написанию дневников и отчетов;

– оказывают методическую и организационную помощь при выполнении ими программы практики;

– ведут учет выхода студентов на практику;

– знакомят руководителей практики от предприятия (организации) с программой по практике и методикой ее проведения, требованиями к практикантам и критериями оценки их работы во время практики;

– контролирует сдачу студентами отчётов по практике и участвует в проведении аттестации по итогам практики;

– организовывает и проводит отчетно-практическую конференцию по результатам практики

Руководство производственной практикой от организации осуществляют лица из числа руководителей и работников организаций, направление деятельности которых соответствует области профессиональной деятельности.

Руководители практики от предприятия (организации) организуют прохождение практики обучающимся следующим образом:

– знакомят с организацией и методами работы на конкретном рабочем месте, с охраной труда и инструктажа по технике безопасности;

– оказывает помощь студентам в сборе, систематизации и анализе информации по предприятию;

– осуществляет консультирование студентов по вопросам, входящим в задание практики, с привлечением специалистов предприятия

– проверяют ведение обучающимся дневника и подготовку отчета о прохождении практики;

– осуществляют постоянный контроль за практикой обучающихся;

– составляют характеристики по освоению общих компетенций, содержащие данные о выполнении программы практики и индивидуальных заданий, об отношении практикантов к работе.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

В период прохождения практики, обучающиеся обязаны вести документацию:

– отчет по практике, который утверждается организацией.

В качестве приложения к дневнику практики обучающийся оформляет графические, фото-, видеоматериалы подтверждающие практический опыт, полученный на практике.

Время прохождения производственной практики определяется графиком учебного процесса и расписанием занятий.

Продолжительность рабочего дня обучающихся при прохождении производственной практики – 6 часов и не более 36 академических часов в неделю.

По результатам практики руководителями практики от организации и от колледжа формируется аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций в период прохождения практики.

Результаты обучения (освоенный практический опыт)	**Формы и методы контроля и оценки результатов обучения**
ВПД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении – установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем; – администрирование автоматизированных систем в защищенном исполнении; – эксплуатация компонентов систем защиты информации автоматизированных систем; – диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении; – *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;*	– экспертное наблюдение выполнения практических заданий; – оценка решения ситуационных задач; – оценка процесса и результатов выполнения видов работ на практике; – защита отчетов по практике; – дифференцированный зачет.

– *установка средств межсетевого экранирования в соответствии с действующими требованиями по защите информации* – *инструктаж пользователей по порядку безопасной работы 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*	
ВПД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами – установка, настройка программных средств защиты информации в автоматизированной системе; – обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации ; – решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; – применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; – учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности; – работа с подсистемами регистрации событий; – выявление событий и инцидентов безопасности в автоматизированной системе. – *определение правил и процедур управления системой защиты информации автоматизированной системы;* – *определение правил и процедур выявления инцидента* – *определение правил и процедур реагирования на инцидент;* – *определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации;* – *выбор и обоснование критериев выбора*	– экспертное наблюдение выполнения практических заданий; – оценка решения ситуационных задач; – оценка процесса и результатов выполнения видов работ на практике; – защита отчетов по практике; дифференцированный зачет.

эффективности функционирования защищенных автоматизированных систем; – *проведение экспертизы состояния защищенности информации автоматизированных систем;* – *проведение предварительных испытаний системы защиты информации автоматизированной системы;* – *уточнение модели угроз безопасности информации автоматизированной системы;* *проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы*	
ВПД 3 Защита информации техническими средствами – установка, монтаж и настройка технических средств защиты информации; – техническое обслуживание технических средств защиты информации; – применение основных типов технических средств защиты информации; – выявление технических каналов утечки информации; – участие в мониторинге эффективности технических средств защиты информации; – диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; – проведение 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; – проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты. – *корректировка конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки, контроля и испытаний;* – *отработка конструкции средств защиты информации на технологичность с учетом стандартов ЕСТД;*	– экспертное наблюдение выполнения практических заданий; – оценка решения ситуационных задач; – оценка процесса и результатов выполнения видов работ на практике; – защита отчетов по практике; – дифференцированный зачет.

– *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;* – *использование основных методов и средств обеспечения информационной безопасности компьютерных средств; применения методов криптографической защиты и аутентификации.*	
ВПД 4 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих – *выполнение требований техники безопасности при работе с вычислительной техникой;* – *организация рабочего места оператора электронно-вычислительных и вычислительных машин;* – *подготовка оборудования компьютерной системы к работе;* – *инсталляция, настройка и обслуживание программного обеспечения компьютерной системы;* – *управление файлами;* – *применение офисного программного обеспечения в соответствии с прикладной задачей;* – *использование ресурсов локальной вычислительной сети;* – *использование ресурсов, технологий и сервисов Интернет;* – *применение средств защиты информации в компьютерной системе.*	– экспертное наблюдение выполнения практических заданий; – оценка решения ситуационных задач; – оценка процесса и результатов выполнения видов работ на практике; – защита отчетов по практике; – дифференцированный зачет.