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. Тупикарова

СОГЛАСОВАНО
Зам. директора по
производственному обучению

«26» 10 2022г.

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

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ 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:

Пушкарева Н.Я., преподаватель компьютерных дисциплин ГБПОУ КК ПСХК, высшей квалификационной категории, математик, преподаватель информатики и ИКТ.

СОДЕРЖАНИЕ

1. **ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ**
2. **РЕЗУЛЬТАТ ПРАКТИКИ**
3. **СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ**
4. **УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ПРАКТИКИ**
5. **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРАКТИКИ**

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1. Место учебной практики в структуре основной профессиональной образовательной программы (далее – ООП)

Программа учебной 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 учебной практики

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

Вид профессиональной деятельности: эксплуатация автоматизированных (информационных) систем в защищенном 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 мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;

– *применять нормативные документы по противодействию технической разведке;*

– *применять нормативные документы для оценки уязвимости;*

– *определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы;*

– *реализовывать правила разграничения доступа персонала к объектам доступа;*

– *настраивать параметры программного обеспечения системы защиты информации автоматизированной системы;*

– *классифицировать каналы утечки информации;*

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

– *реализовывать защитные механизмы в условно-бесплатных и свободно-распространяемых 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 учебной практики

Всего: 13 недель (468 часов), из них:
на учебную практику УП.01 – 2 недели (72 часа);
на учебную практику УП.02 – 2 недели (72 часа);
на учебную практику УП.03 – 6 недель (216 часа);
на учебную практику УП.04 – 3 недели (108 часа).

2. РЕЗУЛЬТАТЫ УЧЕБНОЙ ПРАКТИКИ

Результатом учебной 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
ОК2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	- оперативность поиска и использования информации, необходимой для качественного выполнения профессиональных задач; - широта использования различных источников информации, включая электронные
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	- конструктивность взаимодействия с обучающимися, преподавателями и руководителями практики в ходе обучения и при решении профессиональных задач; - четкое выполнение обязанностей при работе в команде и / или выполнении задания в группе; - соблюдение норм профессиональной этики при работе в команде; - построение профессионального общения с учетом социально-профессионального статуса, ситуации общения, особенностей группы и индивидуальных особенностей участников коммуникации
ОК5. Осуществлять устную и письменную коммуникацию на государственном языке 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	- описывать значимость своей профессии (специальности)

ОК7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	- соблюдение нормы экологической безопасности; - применение направлений ресурсосбережения в рамках профессиональной деятельности по специальности
ОК8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	- использование физкультурно-оздоровительной деятельности для укрепления здоровья, достижения жизненных и профессиональных целей; - применение рациональных приемов двигательных функций в профессиональной деятельности; - пользоваться средствами профилактики подготовленности перенапряжения характерными для данной специальности
ОК9. Использовать информационные технологии в профессиональной деятельности	- применение средств информационных технологий для решения профессиональных задач; - использование современного общего и специализированного программного обеспечения при решении профессиональных задач
ОК10. Пользоваться профессиональной документацией на государственном и иностранном языках	- понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые); - понимать тексты на базовые и профессиональные темы; - участвовать в диалогах на знакомые общие и профессиональные темы; - строить простые высказывания о себе и о своей профессиональной деятельности; - кратко обосновывать и объяснить свои действия (текущие и планируемые); - писать простые связные сообщения на знакомые или интересующие профессиональные темы; - использование в профессиональной деятельности необходимой технической документации

Профессиональных компетенций (ПК):

Вид профессиональной деятельности	КОД	Наименование результатов практики
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	– производит установку типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; – производит адаптацию типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; – производит сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; – знает и использует основные приемы программирования; организует и проводит техническое обслуживание вычислительной техники и других технических средств информатизации.
	ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	– настраивает программно-аппаратные средства защиты информации в компьютерных сетях по заданным правилам; – устраняет неисправности программно - аппаратных средств защиты информации в компьютерных сетях; – использует знания принципов работы автоматизированных систем, операционных систем и сред при настройке средств защиты информации.
	ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с	– обеспечивает работоспособность автоматизированных систем в защищенном исполнении; – обнаруживает неисправности автоматизированных систем в защищенном исполнении;

	требованиями эксплуатационной документации	– устраняет неисправности автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; – осуществляет комплектование автоматизированных систем в защищенном исполнении; – осуществляет конфигурирование и настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем.
	ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении	– распознает задачу и/или проблему в профессиональном контексте; – анализирует задачу и/или проблему и выделяет её составные части; – определяет этапы решения задачи; – выявляет и осуществляет поиск информации, необходимой для решения задачи и/или проблемы; – составляет план действия; определяет необходимые ресурсы; – владеет актуальными методами работы в профессиональной и смежных сферах; – реализует составленный план; – оценивает результат и последствия своих действий, выделяет в нём сильные и слабые стороны
Защита информации в автоматизированных системах программными и программно-	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных	– устанавливает программные и программно- аппаратные средства защиты информации; – настраивает программные и программно- аппаратные средства защиты информации;

аппаратными средствами	средств защиты информации	– применяет программные и программно- аппаратные средства защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных.
	ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	– устанавливает средства антивирусной защиты; настраивает средства антивирусной защиты в соответствии с предъявляемыми требованиями; – устанавливает программные и программно- аппаратные средства защиты информации; – настраивает программные и программно- аппаратные средства защиты информации; – применяет системы контроля и управления доступом для защиты информации; – проверяет выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации
	ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	– проводит диагностику программно-аппаратных средств защиты информации; – устраняет отказы в работе программно- аппаратных средств защиты информации; – обеспечивает работоспособность программно-аппаратных средств защиты информации; – тестирует функции программно-аппаратных средств защиты информации; – восстанавливает работоспособность программных и программно-аппаратных средств защиты информации.

	ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	– применяет симметричные и асимметричные криптографические алгоритмы, и средства шифрования данных; – применяет программные и программно- аппаратные средства для защиты информации в базах данных; – проверяет выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – применяет математический аппарат для выполнения криптографических преобразований; – использует типовые программные криптографические средства, в том числе электронную подпись
	ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	– ведет учёт информации, для которой установлен режим конфиденциальности; – обрабатывает информацию, для которой установлен режим конфиденциальности; – обеспечивает надежное хранение информации, для которой установлен режим конфиденциальности; – передает информацию, для которой установлен режим конфиденциальности, с соблюдением установленных требований; – применяет средства гарантированного уничтожения информации
	ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных	– работает с подсистемами регистрации событий;

	(информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	– выявляет события и инциденты безопасности в автоматизированной системе; – устанавливает программные и программно- аппаратные средства защиты информации; – настраивает программные и программно- аппаратные средства защиты информации; – применяет программные и программно- аппаратные средства защиты информации; – осуществляет мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
Защита информации техническими средствами	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	– устанавливает, производит монтаж и настройку технических средств защиты информации; – производит техническое обслуживание технических средств защиты информации; – применяет основные типы технических средств защиты информации; – применяет технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – знает порядок технического обслуживания технических средств защиты информации; – знает номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам.

	ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	– применяет основные типы технических средств защиты информации; – выявляет технические каналы утечки информации; – участвует в мониторинге эффективности технических средств защиты информации; – производит диагностику, устраняет отказы и неисправности, восстанавливает работоспособности технических средств защиты информации; – применяет технические средства для криптографической защиты информации конфиденциального характера; – применят технические средства для уничтожения информации и носителей информации; – применяет нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – знает 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; – знает порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – знает методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной

	техники на объектах информатизации; – знает номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам.
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	– проводит измерения параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – применяет технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – знает номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – знает структуру и условия формирования технических каналов утечки информации.
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	– проводит измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – выявляет технические каналы утечки информации; – применяет технические средства для защиты информации в условиях применения

	мобильных устройств обработки и передачи данных; – знает номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам.
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации	– производит установку, монтаж и настройку, техническое обслуживание, диагностику, устранять отказы и неисправности, восстанавливает работоспособности инженерно-технических средств физической защиты; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применяет инженерно-технические средства физической защиты объектов информатизации; – знает основные принципы действия и характеристики технических средств физической защиты; – знает основные способы физической защиты объектов информатизации; – знает номенклатуру применяемых средств физической защиты объектов информатизации.
ПК 3.6. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах	– ставит цели, формулирует задачи, связанные с обеспечением корпоративной защиты от внутренних угроз информационной безопасности; – знает объекты компьютерных технологий, используемые в обеспечении корпоративной защиты от внутренних угроз информационной безопасности;

		– знает и применяет технологию анализа и защиты сетевого трафика; – осуществляет развёртывание, настройка и проверка работоспособности VPN -сети на существующей и вычислительной инфраструктуре.
	ПК 3.7. Выявлять и анализировать возможные угрозы информационной безопасности объектов	– анализирует тенденции развития систем обеспечения корпоративной защиты от внутренних угроз информационной безопасности; – применяет знания о корпоративной защите от внутренних угроз информационной безопасности в решении поставленных задач; – применяет классификацию объектов защиты.
	ПК 3.8. Ориентироваться в условиях частой смены технологий в профессиональной деятельности	– применяет понятийный аппарат информационных технологий и особенности терминологии в области корпоративной защиты от внутренних угроз информационной безопасности;
	ПК 3.9. Проводить регламентные работы и фиксировать отказы средств защиты	– применяет базовые составляющие в области развития систем информационной безопасности; – проводит регламентные работы и фиксацию отказов средств защиты.
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*	– правильная подготовка и настройка аппаратного обеспечения персонального компьютера в соответствии с корпоративными стандартами; установка и настройка работы операционной системы с учетом совместимости с аппаратной платформы ПК и корпоративными стандартами.

	ПК 4.2. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах	– создает и управляет текстовыми документами; – создает и управляет электронными таблицами; – создает и управляет презентациями; создает и управляет содержанием баз данных.
	ПК 4.3. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	– осуществляет навигацию по ресурсам сети Интернет; осуществляет поиск и передачу данных с помощью технологий и сервисов Интернета.
	ПК 4.4. Обеспечивать применение средств защиты информации в компьютерной системе	– обеспечивает и правильно применяет средства защиты информации в компьютерной системе

3.СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

3.1. Тематический план учебной практики

Коды формируемых компетенций	Наименование профессионального модуля	Объем времени, отведенный на практику (в неделях, часах)	Сроки проведения
ПК 1.1 – ПК 1.4	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	2 недели, 72 часа	По графику учебного процесса
ПК 2.1 – ПК 2.6	ПМ.02 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*	ПМ.03 Защита информации техническими средствами	6 недель, 216 часов	По графику учебного процесса
ПК 4.1 – ПК 4.4	ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	3 недели, 108 часов	По графику учебного процесса

3.2. Содержание учебной практики

3.2.1. Содержание учебной практики ПМ 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

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 защищенном исполнении	Проведение аудита защищенности автоматизированной системы	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства	МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении Тема 2.2. Администрирование автоматизированных систем	6

		обеспечения отказоустойчивости автоматизированных систем.		
	Установка, настройка и эксплуатация сетевых операционных систем: Windows	Определение операционной системы. Основные понятия. История развития операционных систем. Виды операционных систем. Классификация операционных систем по разным признакам. Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. Исследования в области операционных систем. Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС. Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода. Работа с файлами. Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам. Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	МДК.01.01. Операционные системы Тема 1.1. Основы теории операционных систем Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем Тема 3.2. Операционная система Windows	6

		Виды политик управления доступом и информационными потоками применительно к операционным системам.		
	Установка, настройка и эксплуатация сетевых операционных систем: Linux	Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX.	МДК.01.01. Операционные системы Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	6
	Установка, настройка и эксплуатация сетевых операционных систем: работа с сетевой файловой системой.	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы. Практическая работа №17. Работа с сетевой файловой системой. Практическая работа №18. Работа с серверной ОС.	МДК.01.01. Операционные системы Тема 3.3. Серверные операционные системы	
	Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы. Практическая работа №17. Работа с сетевой файловой системой. Практическая работа №18. Работа с серверной ОС.	МДК.01.01. Операционные системы Тема 3.3. Серверные операционные системы	6
	Организация работ с удаленными хранилищами данных и базами данных	Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых	МДК.01.02 Базы данных Тема 5.1. Архитектуры распределенных баз данных	6

		процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти. *Настройка работоспособности системы управления базами данных.* *Уровни блокировки. Блокировка, как средства разграничения доступа.* Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию. Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД. Средства защиты информации в базах данных.	Тема 5.2. Серверная часть распределенной базы данных 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	

	Организация защищенной передачи данных в компьютерных сетях	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда. Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ.	МДК.01.03. Сети и системы передачи информации Тема 1.2. Принципы передачи информации в сетях и системах связи Тема 1.3. Типовые каналы передачи и их характеристики	6
	Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. Конфигурирование локальных сетей	Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи. Протоколы и интерфейсы управления каналами и сетью передачи данных.	МДК.01.03. Сети и системы передачи информации Тема 2.1. Архитектура и принципы работы современных сетей передачи данных Практическая работа №2. Конфигурирование сетевого интерфейса рабочей станции Практическая работа №3. Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP.	6

	Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. Монтаж ЛВС.	Практическая работа №4. Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне. Практическая работа №5. Диагностика и разрешение проблем сетевого уровня. Практическая работа №6. Диагностика и разрешение проблем протоколов транспортного уровня. Практическая работа №7. Диагностика и разрешение проблем протоколов прикладного уровня.	МДК.01.03. Сети и системы передачи информации Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	6
	Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. Установление и настройка параметров современных сетевых протоколов.	Практическая работа №8. Работа в компьютерных сетях с соблюдением действующих требований по защите информации. Практическая работа №9. Конфигурация и контроль корректности настройки программно-аппаратных средств защиты информации в компьютерных сетях.	МДК.01.03. Сети и системы передачи информации Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	6
	Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей	Практическая работа №10. Мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях.	МДК.01.03. Сети и системы передачи информации Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	6

	Настройка программно-аппаратных средств защиты, в том числе антивирусной защиты в операционных системах по заданным шаблонам	Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ. Обнаружение (предотвращение) вторжений. Контроль (анализ) защищенности информации. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации	МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении Тема 1.5. Содержание учебного материала и порядок эксплуатации АС в защищенном исполнении Тема 1.6. Защита информации в распределенных автоматизированных системах	6
	Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему. *Анализ технического паспорта на защищенную автоматизированную систему.* Практическая работа №29. Оформление основных эксплуатационных документов на автоматизированную систему.	МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении Тема 2.7. Документация на защищаемую автоматизированную систему	4

	Промежуточная аттестация в форме дифференцированного зачета	2
	Всего:	**72 (2 недели)**

3.2.2. Содержание учебной практики ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

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	Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты). Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Автоматизация процесса обработки информации. Понятие автоматизированной	МДК.02.01. Программные и программно-аппаратные средства защиты информации Тема 1.2. Стандарты безопасности. Тема 1.3. Защищенная автоматизированная система.	**6**

		системы. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. Методы создания безопасных систем. Методология проектирования гарантированно защищенных КС. Дискреционные модели. Мандатные модели. *Отсутствие применимых средств реализации мандатного механизма разграничения доступа.*		
	Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности.	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25.Классификация отслеживаемых событий. Особенности построения систем мониторинга Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов. Системы управления событиями информационной безопасности (SIEM).	МДК.02.01. Программные и программно-аппаратные средства защиты информации. Тема 6.1. Мониторинг систем защиты	6

		Обзор SIEM-систем на мировом и российском рынке. Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов *Анализ программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем.* Проведение аудита ЛВС сетевым сканером *Определение методов управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе.*		
	Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности.	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты. Выбор мер защиты информации для их реализации в информационной системе. *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации.*	МДК.02.01. Программные и программно-аппаратные средства защиты информации. Тема 6.2. Изучение мер защиты информации в информационных системах	6

		Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке. Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации.		
	Составление документации по учету, обработке, хранению и передаче конфиденциальной информации.	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты). *Доктрина 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*	МДК.02.01. Программные и программно-аппаратные средства защиты информации Тема 1.2. Стандарты безопасности	6

		от несанкционированного доступа к информации». Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.		
	Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации.	Автоматизация процесса обработки информации. Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. Методы создания безопасных систем *Основные методы снижения затрат на защиту информации в автоматизированных системах.* Методология проектирования гарантированно защищенных КС. Дискреционные модели. Мандатные модели. *Отсутствие применимых средств реализации мандатного механизма разграничения доступа.* Учет, обработка, хранение и передача информации в АИС. *Определение параметров настройки программного обеспечения и системы защиты информации автоматизированной системы.* Ограничение доступа на вход в систему. Идентификация и аутентификация	МДК.02.01. Программные и программно-аппаратные средства защиты информации Тема 1.3. Защищенная автоматизированная система	6

		пользователей. Разграничение доступа. Регистрация событий (аудит). *Реализация правил разграничения доступа персонала к объектам доступа.* Контроль целостности данных. Уничтожение остаточной информации. Управление политикой безопасности. Шаблоны безопасности. *Настройка параметров программного обеспечения системы защиты информации автоматизированной системы.* Криптографическая защита. Обзор программ шифрования данных. *Работа с программой шифрования данных kryptelite.*		
	Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.	Источники дестабилизирующего воздействия на объекты защиты *Сущностные проявления угрозы.* Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию. *Определение причин и условий дестабилизирующего воздействия на информацию.* *Методика выявления способов воздействия на информацию.* Распределение каналов в соответствии с источниками воздействия на информацию *Классификация каналов утечки информации.*	МДК.02.01. Программные и программно-аппаратные средства защиты информации Тема 1.4. Дестабилизирующее воздействие на объекты защиты.	6

	Устранение замечаний по результатам проверки.	Выбор мер защиты информации для их реализации в информационной системе. *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации.* Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке. *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации.*	МДК.02.01. Программные и программно-аппаратные средства защиты информации Тема 6.2. Изучение мер защиты информации в информационных системах	6
	Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.	Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам Доступ к данным со стороны процесса. Особенности защиты данных от изменения. Шифрование. Организация доступа к файлам. *Защита носителей информации.* *Выбор надежного оборудования.* Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	МДК.02.01. Программные и программно-аппаратные средства защиты информации Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	6

	Применение математических методов для оценки качества и выбора наилучшего программного средства.	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов. *Обеспечение безопасности рабочих станций и серверов*. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов. *Обеспечение безопасности рабочих станций и серверов.* Изучение типовых решений для построения VPN на примере VIP Net или других аналогов. *Обеспечение безопасности рабочих станций и серверов.* Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов. *Обеспечение безопасности рабочих станций и серверов.* Изучение функционала и областей применения DLP систем на примере InfoWatch Traffic Monitor или других	МДК.02.01. Программные и программно-аппаратные средства защиты информации Тема 6.2. Изучение мер защиты информации в информационных системах Тема 6.3. Изучение современных программно-аппаратных комплексов.	6

		аналогов. *Обеспечение безопасности рабочих станций и серверов.*		
	Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи *Криптозащита информации в сетях передачи данных. Абонентское шифрование.* *Пакетное шифрование. Защита центра генерации ключей.* Применение различных функций хеширования. *Применение различных функций хеширования.* Анализ особенностей хешей. Применение криптографических атак на хеш-функции. Изучение программно-аппаратных средств, реализующих основные функции ЭП	МДК.02.02. Криптографические средства защиты информации Тема 3.4. Аутентификация данных. Электронная подпись	6
	Определение правил и процедур управления системой защиты информации автоматизированной системы.	*Алгоритмы обмена ключей и протоколы аутентификации.* Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация. Протокол Диффи-Хеллмана для обмена ключами шифрования.	МДК.02.02. Криптографические средства защиты информации Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации Тема 3.6. Криптозащита	6

		Применение протокола Диффи-Хеллмана для обмена ключами шифрования. *Протоколы аутентификации в Windows* *Исследование взаимной аутентификации* *Исследование односторонней аутентификации* Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP. *Применение протоколов WPA, WEP для организации безопасного функционирования беспроводной сети.* *Подбор оборудования для реализации проекта беспроводной сети предприятия.*	информации в сетях передачи данных	
	Определение правил и процедур выявления инцидента и реагирования на него.	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	МДК.02.02. Криптографические средства защиты информации Тема 3.7. Защита информации в электронных платежных системах	4

		Применение аутентификации по одноразовым паролям. *Применение аутентификации по одноразовым паролям.* Реализация алгоритмов создания одноразовых паролей *Применение криптографических протоколов для обеспечения безопасности электронной коммерции.* *Оценка защищенности систем электронных платежей*		
	Промежуточная аттестация в форме дифференцированного зачета			2
	Всего:			**72 (2 недели)**

3.2.3. Содержание учебной практики ПМ 03 Защита информации техническими средствами

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	*Измерение параметров физических полей.* *Определение каналов утечки ПЭМИН.*	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации.	МДК.03.01 Техническая защита информации Тема 2.2. Технические каналы утечки информации	6

		Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика. *Практическая работа № 2. Определение канала утечки информации. Проведение сравнительного анализа каналов.* Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей. *Практическая работа № 4. Расчет наводок в каналах связи.*	Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	
	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Установка и настройка технических	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление. Практическая работа № 8. Организация мероприятий по скрытию речевой информации.	МДК.03.01 Техническая защита информации Тема 3.2. Физические процессы при подавлении опасных сигналов	6

	средств защиты информации.			
	Проведение измерений параметров побочных электромагнитных излучений и наводок.	*Практическая работа № 5. Побочные электромагнитные излучения ПК. Заземление технических средств и подавление информационных сигналов в цепях заземления.* *Практическая работа № 6. Восстановление информации при перехвате побочных электромагнитных излучений и наводок (ПЭМИН). Комплексы измерения ПЭМИН.* *Практическая работа № 7. Съем информации по электрическим каналам утечки информации.*	МДК.03.01 Техническая защита информации Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	6
	Проведение аттестации объектов информатизации.	*Предмет и задачи технической защиты информации. Системный подход при решении задач инженерно-технической защиты объектов. Задачи и требования к способам и средствам защиты информации техническими средствами.* Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути, и способы его проникновения на охраняемый	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации Тема 1.1**.** Цели и задачи физической защиты объектов информатизации Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	6

		объект. Особенности задач охраны различных типов объектов. Практическая работа № 1. Построение модели нарушителя, определение способов его проникновения на объект, на примере образовательной организации. Практическая работа № 2. Построение модели нарушителя, определение способов его проникновения на объект, на примере производственной организации.		
	Монтаж различных типов датчиков.	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия. Практическая работа № 5. *Определение состава инженерных конструкций, необходимых для предотвращения проникновения злоумышленника.* Практическая работа № 6. *Разработка проекта монтажа инженерных конструкций на территории организации.*	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	6
	Проектирование установки системы пожарно-охранной	Практическая работа № 7. Монтаж датчиков пожарной сигнализации. Практическая работа № 8. Монтаж датчиков охранной сигнализации.	МДК.03.02 Инженерно-технические средства физической защиты	6

	сигнализации по заданию и ее реализация.		объектов информатизации Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	
	Применение промышленных осциллографов, частотомеров и генераторов, и другого оборудования для защиты информации. *Рассмотрение системы контроля и управления доступом.*	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Практическая работа № 9. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя. Практическая работа № 10. Рассмотрение принципов устройства, работы и применения средств контроля доступа. *Практическая работа № 11. Особенности построения и размещения СКУД.* *Практическая работа № 12. Периферийное оборудование и носители информации в*	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации Тема 2.2. Система контроля и управления доступом	6

		СКУД. Методы удостоверения личности, применяемые в СКУД. Практическая работа № 13. Сравнительный анализ применения шлюзового турникета и маятниковой двери-шлюза.		
	Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы.	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Состав системы телевизионного наблюдения. Инфракрасные осветители. Детекторы движения. *Дополнительное оборудование систем телевизионного наблюдения.* Практическая работа № 14. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. *Практическая работа № 15. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.* *Практическая работа № 16. Управление системой телевизионного наблюдения с автоматизированного рабочего места.* *Практическая работа № 17. Разработка проекта системы видеонаблюдения для организации.* *Практическая работа № 18. Настройка систем телевизионного наблюдения с*	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации Тема 2.3. Система телевизионного наблюдения. Тема 3.1 Применение инженерно-технических средств физической защиты	6

		учетом специфики деятельности организации. Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. *Особенности выбора инженерно-технических средств физической защиты периметров протяженных объектов. Особенности монтажа.* Особенности организации пропускного режима на КПП.		
	Выполнение звукоизоляции помещений системы зашумления.	*Номенклатура применяемых средств обнаружения (вибрационные, магнитометрические, объектовые).* Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. *Быстро развертываемые комплексы ТСО: состав, отличительные особенности, преимущества от внедрения.* *Практическая работа № 5. Определение состава инженерных конструкций, необходимых для предотвращения проникновения злоумышленника.*	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	6

	Реализация защиты от утечки по цепям электропитания и заземления.	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия. *Организация охраны объектов с применением технических средств воздействия.* *Практическая работа № 23. Мониторинг эффективности технических средств воздействия для гражданских организаций* *Практическая работа № 24. Определение эффективности технических средств воздействия для гражданских организаций.* *Практическая работа № 25. Испытание на устойчивость технических средств охраны.* *Практическая работа № 26. Разработка проекта применения технических средств воздействия для образовательной организации.*	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации Тема 2.5 Система воздействия	6
	Разработка организационных и технических мероприятий по заданию преподавателя.	*Практическая работа № 27. Разработка структурной схемы оборудования инженерно-технических средств физической защиты.* *Практическая работа № 28. Представление моделей объектов информационной безопасности.*	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации Тема 3.1 Применение инженерно-технических средств физической защиты	6
	Разработка основной документации по	*Нормативная документация использования технических средств физической защиты.*	МДК.03.02 Инженерно-	6

	инженерно-технической защите информации.	*Единая система конструкторской документации. Единая система технологической документации.* *Порядок применения устройств отображения и документирования информации. Управление системой воздействия.* *Практическая работа № 29. Разработка спецификации оборудования физической защиты объекта.*	технические средства физической защиты объектов информатизации Тема 3.1 Применение инженерно-технических средств физической защиты	
	Конфигурация сетевой инфраструктуры: настройка хост машины, сетевого окружения, виртуальных машин, и т.п.	*Сетевое окружение. Сетевые протоколы. Методы выявления и построения путей движения информации в организации. Подходы к построению сети. Настройка сетевых устройств для эффективного взаимодействия. Типы сетевых устройств. Разнообразие операционных систем, их возможности с точки зрения использования и развертывания компонент систем защиты от внутренних угроз. Процесс выбора драйверов и программного обеспечения для различных аппаратных средств и операционных систем.* *Этапы установки систем корпоративной защиты от внутренних угроз. Назначение компонент системы корпоративной защиты от внутренних угроз.* *Технологии программной и аппаратной виртуализации. Конфигурация сетевой инфраструктуры: настройка хост*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.2**.** *Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз*	6

		машины, сетевого окружения, виртуальных машин, и т.п. *Практическая работа № 1. Конфигурация сетевой инфраструктуры: настройка хост машины, сетевого окружения, виртуальных машин.* *Практическая работа № 2. Установка сервера Traffic Monitor.* *Практическая работа № 3. Установка лицензии Traffic Monitor. Установка Базы данных.* *Практическая работа № 4 Установка подсистемы Краулер. Установка рабочего места Офицера Безопасности. Создание пользователя виртуальной машины IWDM (Офицер Безопасности). Настройка рабочего места Офицера Безопасности. Конфигурация сетевой инфраструктуры: настройка хост машины, сетевого окружения, виртуальных машин.*		
	Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развёртывании и настройке системы корпоративной защиты от внутренних угроз.	*Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развертывании и настройке.* *Практическая работа № 5. Установка серверной части Info Watch Device Monitor. Установка рабочего места потенциального нарушителя. Настройка сетевого взаимодействия. Создание пользователя*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.2**.** *Установка, конфигурирование и устранение неисправностей в системе*	6

		виртуальной машины Agent1 (Потенциальный нарушитель). Настройка рабочего места на машине Agent1. Установка DM Client. *Практическая работа № 6. Работа в Консоли управления Device Monitor. Авторизация и соединение с сервером InfoWatch Device Monitor. Главное окно Консоли управления (DM). Разделы Консоли управления (DM).*	*корпоративной защиты от внутренних угроз*	
	Установка и настройка агентского мониторинга. Проведение синхронизация с LDAP-сервером.	*Установка и настройка агентского мониторинга. Синхронизация с LDAPсервера.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.2**.** *Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз*	6
	Запуск системы корпоративной защиты от внутренних угроз, проверка ее работоспособности.	*Практическая работа № 9. Создание подразделений организации с использованием AD сервера. Синхронизация каталога пользователей и компьютеров.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.3. *Исследование (аудит) организации с*	6

			целью защиты от внутренних угроз	
	Проведение имитации процесса утечки конфиденциальной информации в системе.	*Угрозы информационной безопасности. Исследование (аудит) организации на основании полученных материалов («модели организации»), обследование корпоративных информационных систем Определение объектов защиты. Перечень субъектов, персон, роли пользователей, права доступа Практическая работа № 7. Изучение структуры организации. Обследование корпоративных информационных систем Практическая работа № 8. Добавление роли Администратора системы. Добавление роли пользователя для проведения аудита*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.3. *Исследование (аудит) организации с целью защиты от внутренних угроз*	6
	Настройка защищенного домена, групповых политик AD. Создание и установка цифровых сертификатов.	*Практическая работа № 9. Создание подразделений организации с использованием AD сервера. Синхронизация каталога пользователей и компьютеров.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.3. *Исследование (аудит) организации с целью защиты от внутренних угроз*	6
	Настройка защищенного соединения между элементами сетевой инфраструктуры: SSH, HTTPS и т.п.	*Сетевое окружение. Сетевые протоколы. Методы выявления и построения путей движения информации в организации. Подходы к построению сети. Настройка*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности	6

		сетевых устройств для эффективного взаимодействия. *Настройка рабочего места Офицера Безопасности. Конфигурация сетевой инфраструктуры: настройка хост машины, сетевого окружения, виртуальных машин.*	Тема 1.2. *Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз*	
	Исследование (аудит) организации с целью защиты от внутренних угроз.	*Угрозы информационной безопасности. Исследование (аудит) организации на основании полученных материалов («модели организации»), обследование корпоративных информационных систем Определение объектов защиты. Перечень субъектов, персон, роли пользователей, права доступа Практическая работа № 7. Изучение структуры организации. Обследование корпоративных информационных систем Практическая работа № 8. Добавление роли Администратора системы. Добавление роли пользователя для проведения аудита*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.3. *Исследование (аудит) организации с целью защиты от внутренних угроз*	6
	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз.	*Работа с интерфейсом управления системы корпоративной защиты информации. Раздел Технологии.* *Работа с объектами защиты в интерфейсе управление системой.* *Практическая работа № 10. Работа с категориями и терминами.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.4**.** *Разработка политик безопасности в системе*	6

		Практическая работа № 11. Работа с текстовыми объектами. *Практическая работа № 12. Работа с эталонными документами.*	*корпоративной защиты информации от* *внутренних угроз*	
	Разработка новых и/или модификация существующих политик безопасности, перекрывающие каналы передачи данных и возможные инциденты.	*Работа с интерфейсом управления системы корпоративной защиты информации. Раздел Технологии.* *Работа с объектами защиты в интерфейсе управление системой.* *Политика безопасности. Модификация политики безопасности в системе IWTM.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.4. *Разработка политик безопасности в системе корпоративной защиты информации от* *внутренних угроз*	6
	Разработка или/и модификация объектов защиты, категорий, технологий защиты в DLP-системе и т.п.	*Работа с интерфейсом управления системы корпоративной защиты информации. Раздел Технологии.* *Работа с объектами защиты в интерфейсе управление системой.* *Практическая работа № 12. Работа с эталонными документами.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.4. *Разработка политик безопасности в системе корпоративной защиты информации от* *внутренних угроз*	6

	Использование различных технологий защиты: печатей, бланков, графических объектов, баз данных и т.п. Занесение политик информационной безопасности в DLP систему.	*Работа с интерфейсом управления системы корпоративной защиты информации. Раздел Технологии. Работа с объектами защиты в интерфейсе управление системой. Практическая работа № 13. Работа с бланками. Практическая работа № 14. Работа с печатями. Практическая работа № 15. Работа с выгрузками. Практическая работа № 16. Работа с графическими объектами.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.4. *Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз*	6
	Модификация политик безопасности в системе IWTM в соответствие с получаемыми на практике данными перехвата.	*Политика безопасности. Модификация политики безопасности в системе IWTM. Общие действия при управлении схемой безопасности. Просмотр действующей версии схемы безопасности. Редактирование и обновление схемы безопасности. Экспорт/импорт конфигурации. Практическая работа № 20. Добавление новой политики: создание политики защиты данных, создание политики защиты данных на агентах, создание политики контроля персон.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.4. *Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз* Тема 1.5. *Технологии агентского мониторинга*	6
	Применение политики для контроля трафика,	*Состав серверной части InfoWatch Device Monitor: база данных, сервер InfoWatch*	МДК.03.03 Корпоративная защита	6

	выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизирование числа выявленных инцидентов безопасности. Работа с интерфейсом управления системы корпоративной защиты информации.	*Device Monitor, консоль управления InfoWatch Device Monitor. Общие принципы работы с Консолью управления InfoWatch Device Monitor (DM): авторизация и соединение с сервером InfoWatch Device Monitor, главное окно Консоли управления, разделы Консоли управления. Способы установки Агента Device Monitor на рабочие станции: Локальная установка, удаленная, через задачи распространения в Консоли управления, установка с помощью средств распространения программного обеспечения. Практическая работа № 22. Учетные записи пользователей Консоли управления (DM). Добавление учетной записи Консоли управления. Редактирование учетной записи Консоли управления (DM). Блокирование и разблокирование учетной записи Консоли управления (DM). Удаление учетной записи Консоли управления (DM). Практическая работа № 23. Роли пользователей Консоли управления (DM). Добавление роли пользователя Консоли управления. Редактирование роли пользователя. Удаление роли пользователя.*	от внутренних угроз информационной безопасности Тема 1.5. *Технологии агентского мониторинга*	

	Применение технологии анализа и защиты сетевого трафика. *Применение технологии агентского мониторинга.*	*Управление схемой безопасности. Организация схемы безопасности. Политики безопасности и правила (DM). Сотрудники и группы сотрудников. Компьютеры и группы компьютеров. Загрузка схемы безопасности на контролируемые компьютеры. Общие действия при управлении схемой безопасности. Просмотр действующей версии схемы безопасности. Редактирование и обновление схемы безопасности. Экспорт/импорт конфигурации. Настройка схемы безопасности. Политики безопасности (DM). Просмотр политик безопасности (DM). Создание и настройка политики безопасности (DM). Редактирование политики безопасности (DM). Удаление политики безопасности (DM).*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.5. *Технологии агентского мониторинга*	6
	Разработка и применение политики агентского мониторинга для работы с носителями и устройствами. *Разработка и применение политики агентского мониторинга для работы с файлами.*	*Практическая работа № 30. Правило (DM) для Mail Monitor. Правило для Network Monitor. Правило для Print Monitor. Правило для ScreenShot Control Monitor. Правило для ScreenShot Monitor.* *Практическая работа № 31. Белые списки устройств. Просмотр сведений о белых списках. Добавление белого списка. Установка периода действия записи.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.5. *Технологии агентского мониторинга*	6

		Редактирование белого списка. Удаление белого списка.		
	Работа с исключениями из перехвата. Защита узлов. Групповые политики AD, файерволы и т.п.	*Практическая работа № 32. Приложения. Создание и изменение списка приложений. Добавление приложения в список автоматически. Добавление приложения в список вручную. Экспорт протокола приложения.* *Практическая работа № 33. Временный доступ сотрудника к сети. Временный доступ сотрудника к устройствам.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.5. *Технологии агентского мониторинга*	6
	Проведение анализа выявленных инцидентов. Подготовка отчётов о нарушениях. Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов. Проведение классификации уровня угроз инцидентов.	*Создание тестовой политики в IWTM. Создание тестовой политики в DM. Работа в тематических разделах Сводка, События интерфейса Консоли управления Traffic Monitor. Отчеты интерфейса Консоли управления Traffic Monitor.* *Практическая работа № 37. Создание тестовой политики в IWTM.* *Практическая работа № 38. Создание тестовой политики в DM.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.6**.** *Анализ выявленных инцидентов*	6
	Разработка плана по дальнейшему расследованию выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу.	*Практическая работа № 39. Генерация событий для тестирования политики.* *Практическая работа №40. Работа с отчетами. Создание и просмотр отчетов. Создание папки с отчетами.* *Практическая работа № 41. Создание и настройка виджета. Просмотр готовых отчетов.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 1.6**.** *Анализ выявленных инцидентов*	6

	Развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре.	*Технология защиты информации VipNet. Структура сети VipNet. Типы связей в сети VipNet. Управляющий драйвер. Виртуальные адреса сети VipNet.* *Основные компоненты сети VipNet. Базовые модули VipNet. VipNet Администратор. VipNet Координатор. VipNet Клиент. VipNet Policy Manager. VipNet Центр управления сетью (ЦУС). Основные функциональные возможности. Архитектура программы VipNet ЦУС. Взаимодействие с программой VipNet Удостоверяющий и ключевой центр и с программой VipNet Registration Point. Связи между объектами сети VipNet. Роли сетевых узлов. Справочники и ключи VipNet. Топология сети: основные понятия сетевого уровня. Функции координатора в защищенной сети VipNet. Туннелирование. Принципы осуществления соединений в сети VipNet. Организация межсетевого взаимодействия.* *Практическая работа № 42. Планирование защищенной сети* VipNet. *Проработка схемы сети.* *Практическая работа № 43. Подготовка виртуального стенда. Создание и настройка виртуальных машин.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 2.1. *Программные решения построения и управления виртуальными и защищенными сетями* Тема 2.2**.** *Базовый программный комплекс VipNet Administrator*	6
	Развёртывание, настройка и проверка	*Практическая работа № 44. Установка и первичная настройка компонентов*	МДК.03.03 Корпоративная защита	6

	работоспособности IDS-системы на существующей и вычислительной инфраструктуре.	*программного обеспечения VipNet Administrator.* *Практическая работа № 45. Создание структуры защищенной сети.* *Практическая работа № 46. Создание межсерверных каналов и связей.*	от внутренних угроз информационной безопасности Тема 2.2. *Базовый программный комплекс VipNet Administrator*	
	Работа с узлами и пользователями VPN. Компрометация узлов, ключей, пользователей VPN. Восстановление связи. Обновление ключевой информации VPN.	*Ключевая система в ПО VipNet. Формирование ключевой информации в VipNet. Мастер-ключи. Формирование ключей при первоначальном развертывании сети. Дистрибутивы ключей. Ключи пользователя. Ключи узла. Компрометация ключей. Резервный набор персональных ключей. Межсетевые мастер-ключи. Электронная подпись. Сертификат ключа проверки ЭП.* *Практическая работа № 47. Первый запуск программы ViPNet Удостоверяющий и ключевой центр. Выдача дистрибутивов ключей.* *Практическая работа № 48. Настройка резервного копирования и восстановление данных в ПО ViPNet Administrator.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 2.2. *Базовый программный комплекс VipNet Administrator*	6
	Межсетевое взаимодействие и туннелированные VPN.	*ПАК VipNet Coordinator HW4. Назначение. Функциональные возможности. Общий обзор базовой линейки программно-аппаратных комплексов VipNet. Администрирование. Сценарии применения ПАК.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 2.6**.** *Программно-аппаратный комплекс*	6

		Программное обеспечение ПАК VipNet Coordinator HW. Инсталляция ПО. Верификация образа ПО. Запись образа ПО на носитель. Развертывание ключевых баз. Работа с командной строкой. Общие принципы работы с конфигурационными файлами. *Практическая работа № 55. Межсетевое взаимодействие. Установка VipNet Coordinator в качестве межсетевого шлюза. Первоначальная настройка межсетевого взаимодействия.* *Практическая работа № 56. Модификация межсетевого взаимодействия.* *Практическая работа № 57. Firewall. Фильтры по умолчанию.* *Практическая работа № 58. Фильтрация незащищенного локального трафика.* *Практическая работа № 59. Фильтрация незащищенного транзитного трафика.* *Практическая работа № 60. Включение антиспуфинга.* *Практическая работа № 61. Настройка трансляции сетевых адресов.* *Практическая работа № 62. Фильтрация защищенного трафика.* *Практическая работа № 63. Настройка Автономного режима.* *Практическая работа № 64. Настройка полутуннеля.*	*(ПАК) Координатор VipNet HW4*	

	Применение централизованных политик безопасности VPN. Защита рабочих мест.	*Практическая работа № 66. Настройка расписания в правилах фильтрации.* *Практическая работа № 67. Агрегация каналов.* *Практическая работа № 68. Включение и настройка протокола динамической маршрутизации OSPF.* *Практическая работа № 69. Настройка кластера горячего резервирования.* *Практическая работа № 70. Криптопровайдер* VipNet CSP. Работа с сертификатами. Работа с ЭП. *Практическая работа № 71. Работа с приложениями VipNet. Установка прямого взаимодействия по каналу MFTP.* *Практическая работа № 72. Настройка автопроцессинга в программе ViPNet Деловая почта.*	МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности Тема 2.6. *Программно-аппаратный комплекс (ПАК) Координатор VipNet HW4*	4
	Промежуточная аттестация в форме дифференцированного зачета			2
	Всего:			**216 (6 недель)**

3.2.4. Содержание учебной практики ПМ 04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

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	*Изучение структуры ЭВМ, системного блока ПК. Использование устройств ввода – вывода.*	*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. Поколения и типы ЭВМ. Понятие об архитектуре ЭВМ. Системный блок и его составляющие. Периферийные устройства, их предназначение и разновидности. Устройства ввода-вывода информации. Назначение, виды, характеристики, принцип действия.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 1.1. *Устройства компьютерной системы*	6
	Работа с дополнительными внешними устройствами ПК.	*Периферийные устройства, их предназначение и разновидности. Устройства ввода-вывода информации. Назначение, виды, характеристики, принцип действия. Носители информации.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 1.1. *Устройства*	6

			компьютерной системы	
	Установка операционной системы, настройка пользовательского интерфейса операционной системы.	*Основные понятия операционных систем (ОС). Основные функции. Установка операционной системы. Настройки операционных систем.* *Практическая работа № 1. Настройка среды операционной системы. Работа с рабочим столом. Работа с окнами программ и диалоговыми окнами.* *Практическая работа №2. Работа с файловой структурой. Работа с папками, файлами, ярлыками.* *Практическая работа №3. Работа с прикладными стандартными программами. Внедрение и связывание объектов.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 1.2. *Операционная система*	6
	Работа с программами-архиваторами.	*Архивирование данных.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 1.3. *Сервисное программное обеспечение и защита информации*	6
	Работа с программами-утилитами.	*Сервисные программы. Программы обслуживания магнитных дисков.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ	6

			Тема 1.3. *Сервисное программное обеспечение и защита информации*	
	Антивирусная защита своего рабочего места.	*Антивирусная защита.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 1.3. *Сервисное программное обеспечение и защита информации*	6
	Установка программного обеспечения.	*Защита информации.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 1.3. *Сервисное программное обеспечение и защита информации*	6
	Создание, редактирование, форматирование текстовых документов в среде MS Word. Применение шрифтов и их атрибутов, выравнивание текста;	*Офисные приложения MS Office. Основные виды программ.* *Текстовые редакторы. Текстовый процессор MS Word, его назначение, возможности. Интерфейс MS Word. Режимы просмотра документа. Основные*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ	6

	создание списков, нумерация страниц;	*операции по работе с документами. Виды форматирования.* *Практическая работа №7. Настройка окна документа. Настройка панели быстрого доступа. Создание нового документа. Открытие существующего документа. Сохранение документа в разных форматах. Закрытие документа. Работа с документами, созданными в предыдущих версиях MS Word. Выделение текста. Удаление текста. Перемещение по тексту. Копирование и перемещение текста. Отмена действия ошибочных команд. Перенос слов по слогам. Задание параметров страницы. Разделение окна на две области.* *Практическая работа №8. Форматирование символов: шрифт, размер шрифта, цвет шрифта. Установка интервалов между символами, смещение символов относительно строки. Интервалы между абзацами. Межстрочные интервалы. Граница абзаца. Установка границ страницы. Разбиение текста на колонки. Установка переноса по слогам.*	Тема 2.1. *Технология обработки текстовой информации*	
	Создание таблиц, диаграмм, внедрение объектов. Поля. Создание электронного документа.	*Представление информации в табличной форме. Оформление таблиц. Вычисления в таблицах с помощью формул. Списки. Математические формулы. Работа с графикой в документах.* *Практическая работа №9. Создание и редактирование таблиц. Оформление таблиц. Вычисления в таблицах.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 2.1. *Технология*	6

		Практическая работа №10. Списки. Создание списков разного вида. Работа со стилями. Шаблоны. Вставка математических формул. *Практическая работа №11. Работа с многостраничным документом. Установка разрыва страницы. Номера страниц. Удаление номеров страниц. Работа с колонтитулами. Вставка и удаление сноски. Создание, обновление и удаление оглавления.* *Практическая работа №12. Работа с графическими изображениями. Вставка графического объекта. Работа с полотном. Редактирование рисунков, фигур, объектов WordArt, SmartArt. Вставка рисунков в текст. Работа с группой объектов.*	*обработки текстовой информации*	
	Настройка и параметры MS Excel. Использование различных способов адресации, ввод и редактирование формул. Оформление разбивки рабочего листа, различные параметры форматирования.	*Назначение MS Excel, его возможности. Интерфейс MS Excel. Основные понятия. Ввод текстовых и числовых данных. Вычисления по формулам. Встроенные функции. Форматирование данных и ячеек. Вставка графических объектов. Вставка, редактирование и оформление диаграммы.* *Практическая работа №13. Основные приемы работы с данными и формулами. Создание новой книги. Открытие, сохранение книги. Перемещение по листу. Выделение элементов таблицы. Работа с листами рабочей книги. Работа со строками и столбцами. Ввод и редактирование данных. Использование*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 2.2. *Технология обработки числовой информации*	6

		автозаполнения. Установка специальных форматов данных. *Практическая работа №14. Создание формул с использованием ссылки на ячейки. Автосуммирование.* *Практическая работа №15. Вставка встроенных функций.*		
	Функции MS Excel, работа с группой рабочих листов. Использование поименованных диапазонов, констант, формул. Создание диаграмм, форматирование, перемещение, масштабирование, редактирование диаграмм. Встроенные функции.	*Вычисления по формулам. Встроенные функции. Форматирование данных и ячеек. Вставка графических объектов. Вставка, редактирование и оформление диаграммы.* *Практическая работа №16. Основные приемы форматирования данных и ячеек. Построение, редактирование и оформление диаграмм и графиков.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 2.2. *Технология обработки числовой информации*	6
	Работа со списками. Обмен данными между текстовым процессором и электронной таблицей.	*Практическая работа №17. Основные приемы работы со списками: поиск, замена, сортировка. Выбор данных с помощью автофильтра.* *Практическая работа №18. Связь между рабочими листами. Копирование данных из книги Excel в документ Word без установки связи, с установкой связи. Внедрение таблицы Excel в документ Word.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 2.2. *Технология обработки числовой информации*	6
	Проектирование и создание базы данных, создание таблиц, ввод и редактирование данных, изменение свойств полей,	*Система управления базами данных MS Access. Назначение и возможности MS Access. Основные термины реляционных баз данных. Структура базы данных.*	МДК.04.01. Оператор электронно-вычислительных и	6

	добавление записей. Межтабличные связи, создание связи, задание поля подстановок, условий целостности.	*Объекты СУБД MS Access. Интерфейс MS Access. Главное окно MS Access. Разработка элементов базы данных. Таблицы. Запросы. Формы. Отчеты. Многотабличные базы данных. Типы связей.* *Практическая работа №19. Создание новой базы данных. Открытие базы данных. Создание таблицы в режиме конструктора. Ввод и редактирование данных. Форматирование данных.*	вычислительных работ Тема 2.3. *Технология работы с базами данных*	
	Создание и использование запросов. *Создание форм, кнопочная форма. Создание и печать отчетов.*	*Практическая работа №20. Создание запросов к базе данных.* *Практическая работа №21. Создание форм. Создание отчетов.* *Практическая работа №22. Создание многотабличной базы данных.* *Практическая работа №23. Создание подчиненных форм.* *Практическая работа №24.* Создание элементов управления с использованием макросов.	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 2.3. *Технология работы с базами данных*	6
	Мультимедийные технологии обработки и представления информации, создание презентаций с помощью MS Power Point. *Редактирование и форматирование презентации.*	*Подготовка презентаций с помощью MS PowerPoint. Назначение и возможности MS PowerPoint. Создание слайда. Оформление презентации. Эффекты анимации. Подготовка к показу и печать презентации.* *Практическая работа №25. Создание новой презентации, ввод текста, вставка рисунка, установка эффектов анимации.* *Практическая работа №26. Добавление к презентации слайда и выбор новой разметки слайда. Добавление к*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 2.4. *Технология работы с мультимедийными презентациями*	6

		презентации слайдов с текстом и графикой. Создание итогового слайда (содержание презентации).		
	Оформление презентации. Использование анимации текста, диаграмм и графических объектов, звукового сопровождения и видеоклипов в оформлении презентации. *Настройка презентации. Демонстрация презентации.*	*Подготовка презентаций с помощью MS PowerPoint. Назначение и возможности MS PowerPoint. Создание слайда. Оформление презентации. Эффекты анимации. Подготовка к показу и печать презентации.* *Практическая работа №27. Основные приемы работы со звуком. Вставка звуковых файлов. Задание непрерывного воспроизведения звука.* *Практическая работа №28. Вставка фильма. Изменение способа запуска. Установка временной задержки, продолжение воспроизведения. Применение действий с фильмами* *Практическая работа №29. Создание кнопок. Добавление к кнопкам действий.* *Практическая работа №30. Запуск показа слайдов. Печать раздаточных материалов. Подготовка презентации для демонстрации на другом компьютере.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 2.4. *Технология работы с мультимедийными презентациями*	6
	Настройка локальной сети. Настройка подключения Интернет, поиск и просмотр информации, копирование и сохранение нужных файлов.	*Понятие о компьютерной сети. Назначение компьютерной сети. Типы сетей. Топология сети. Передача данных по сети. Назначение протоколов. Понятие глобальной компьютерной сети. Всемирная паутина WWW. Поиск информации в Интернете. Работа с электронной почтой.* *Практическая работа №31. Работа в сети Интернет. Основные приемы*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 3.1. *Ресурсы сетевых технологий и сервисов*	6

		работы в браузере. Навигация в сети Интернет. *Практическая работа №32. Работа с поисковыми системами. Сохранение информации с Web-страницы в виде текстового файла.*	*компьютерных сетей*	
	Работа с электронной почтой, отправка информации по требуемому адресу.	*Практическая работа №33. Работа с электронной почтой. Регистрация почтового ящика. Создание и отправка писем. Ответ на письмо. Вложенные файлы. Пересылка. Удаление писем.*	МДК.04.01. Оператор электронно-вычислительных и вычислительных работ Тема 3.1. *Ресурсы сетевых технологий и сервисов компьютерных сетей*	4
	Промежуточная аттестация в форме дифференцированного зачета			2
	Всего:			**108** **(3 недели)**

4. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к документации, необходимой для проведения практики

– программа учебной практики;
– приказ о педагогической нагрузке преподавателей;
– график проведения практики.

4.2. Требования к материально-техническому обеспечению

Программа учебной практики реализуется в специализированном компьютерном классе колледжа, оборудованным 15 рабочими местами и одним рабочим местом преподавателя. Каждое рабочее место оснащено персональными компьютером, подключенным к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет, методической документацией и лицензионным программным обеспечением:

– операционные системы;
– сервисные программы (в составе операционной системы или др.);
– программы-архиваторы;
– интегрированное офисное приложение, включающее текстовый редактор, электронные таблицы, систему управления базами данных, программу подготовки презентаций, программу подготовки публикаций;
– браузер (входит в состав операционных систем или др.);
– антивирусный программный комплекс;
– программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности;
– программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;
– средства уничтожения остаточной информации в запоминающих устройствах;
– программные средства криптографической защиты информации;
– *программный комплекс VipNet;*
– *программный комплекс Info Watch Traffic Monitor.*

Компьютерный класс оснащается МФУ (принтером),

4.3. Перечень учебных изданий, Интернет ресурсов, дополнительной литературы

4.3.1. 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.
3. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2018
4. 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.
5. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2014.

6. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., исп. 2014.
7. 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.
8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2019. – 416 с.
9. Киселев С.В. Оператор ЭВМ: учеб. пособие для студ. учреждений сред. проф. образования /. – 7-е изд., исп. – М.: Издательский центр «Академия», 2020.
10. Коньков, К. А. Устройство и функционирование ОС Windows. Практикум к курсу Операционные системы. /Учебное пособие // К.А. Коньков. М.: Бином, Лаборатория знаний Интуит, 2018.
11. Костров Б. В., Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2016.
12. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. - 2-е изд.- М.: Горячая линия-Телеком, 2014.
13. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012
14. Мельников Д. Информационная безопасность открытых систем. - М.: Форум, 2013.
15. Михеева Е.В. Информационные технологии в профессиональной деятельности. – М.: Издательский центр «Академия», 2021.
16. Михеева Е.В. Практикум по информационным технологиям в профессиональной деятельности. – М.: Издательский центр «Академия», 2021.
17. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: в 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2018. – 184 с.
18. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: в 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2018. – 172 с.
19. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2015.
20. 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
21. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.
22. Синицын С.В., Батаев А.В., Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2016.
23. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
24. Струмпэ Н.В. Оператор ЭВМ. Практические работы: учеб. пособие для нач. проф. образования / – 6-е изд., стер. – М.: Издательский центр «Академия», 2013.

25. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2013.
26. Федотова Е.Л. Информационные технологии в профессиональной деятельности. - М: ФОРУМ, 2021. Режим доступа: http://znanium.com
27. Филимонова Е.В. Информационные технологии в профессиональной деятельности. - М: КноРус,2021. Режим доступа: https://www.book.ru
28. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2019

4.3.2. Дополнительные источники

1. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.
2. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2016. – 224 с.
3. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. - СПб: Питер, 2016 - 703 с.
4. ГубенковА.А. Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2019. - 88 с.
5. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы – М.: Бином, 2011. – 1024 с.
6. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бином, 2021. – 704 с.
7. Жмакин А. П. Архитектура ЭВМ: учеб. пособие для вузов / А. П. Жмакин. - 2-е изд., перераб. и доп. - СПб: БХВ-Петербург, 2018. - 352 с.: ил. - (Учебная литература для вузов)
8. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник. -М.: Горячая линия-Телеком. 2018
9. Кофлер М., Linux. Полное руководство – Питер, 2021. – 800 с.
10. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие. -М.: Радио и связь, 2008
11. 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.
12. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.
13. 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.
14. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб. пос. для студентов СПО – М.: Форум, 2013. – 544 с.
15. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. – М.: Академия, 2006. – 240 с.
16. 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

17. Руссинович М., Соломон Д., Внутреннее устройство Microsoft Windows. Основные подсистемы операционной системы – Питер, 2014. – 672 с.
18. Сафонов, В.О. Основы современных операционных систем: учебное пособие. М.: Бином. Лаборатория знаний, 2014. – 583 с.
19. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008. – 368 с.
20. Уваров, С. 500 лучших программ для вашего компьютера (2 CD) / С. Уваров. СПб: Питер, 2009. –·320 с.
21. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
22. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
23. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
24. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
25. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
26. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
27. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
28. 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».
29. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
30. 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.
31. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
32. 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.
33. 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.
34. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
35. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
36. Требования о защите информации, содержащейся в информационных системах

общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
37. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
38. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
39. 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.
40. 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».
41. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
42. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
43. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
44. 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
45. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
46. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
47. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
48. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
49. 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
50. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
51. 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

52. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
53. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
54. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
55. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
56. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
57. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
58. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
59. 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.
60. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
61. 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.
62. 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.
63. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
64. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
65. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
66. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
67. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
68. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
69. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
70. Методические рекомендации по технической защите информации, составляющей

коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

4.3.3. Электронные источники

1. Базы данных, информационно-справочные и поисковые системы: www.fstec.ru, www.gost.ru/wps/portal/tk362
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. Российский биометрический портал www.biometrics.ru
6. Сайт журнала Информационная безопасность http://www.itsec.ru
7. Сайт Научной электронной библиотеки www.elibrary.ru
8. Справочно-правовая система «Гарант» www.garant.ru
9. Справочно-правовая система «Консультант Плюс» www.consultant.ru
10. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
11. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
12. Федеральный портал «Российское образование www.edu.ru
13. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

4.4. Требования к руководителям учебной практики от образовательного учреждения

Руководство учебной практикой осуществляют преподаватели дипломированные специалисты — преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин.

Квалификация педагогических работников образовательной организации должна отвечать квалификационным требованиям, указанным в профессиональном стандарте «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования», утвержденном приказом Министерства труда и социальной защиты Российской Федерации от 8 сентября 2015 г. № 608н.

Педагогические работники, привлекаемые к реализации образовательной программы, должны получать дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях, направление деятельности которых соответствует области профессиональной деятельности, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ УЧЕБНОЙ ПРАКТИКИ

Результаты обучения (освоенный практический опыт)	**Формы и методы контроля и оценки результатов обучения**
ВД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении – 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*	– экспертное наблюдение выполнения практических заданий; – оценка решения ситуационных задач; – оценка процесса и результатов выполнения видов работ на практике; – дифференцированный зачет.

средства защиты информации в компьютерных сетях; – *определения состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях.*	
ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами – 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*	– экспертное наблюдение выполнения практических заданий; – оценка решения ситуационных задач; – оценка процесса и результатов выполнения видов работ на практике; – дифференцированный зачет.

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.*	
ВД 3 Защита информации техническими средствами – 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;	– экспертное наблюдение выполнения практических заданий; – оценка решения ситуационных задач; – оценка процесса и результатов выполнения видов работ на практике; – дифференцированный зачет.

– 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.*	
ВД 4 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих – *выполнения требований техники безопасности при работе с вычислительной техникой;* – *организации рабочего места оператора электронно-вычислительных и вычислительных машин;* – *подготовки оборудования компьютерной системы к работе;*	– экспертное наблюдение выполнения практических заданий; – оценка решения ситуационных задач; – оценка процесса и результатов выполнения видов работ на практике; – дифференцированный зачет.

– *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.*	