**Департамент образования Ярославской области**
**Государственное профессиональное образовательное учреждение Ярославской области**

**Переславский колледж им. А. Невского**

**УТВЕРЖДАЮ**

Директор ГПОУ ЯО Переславский колледж им. А. Невского

_____Е. В. Белова

«___» _____2018 г.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

2018

Разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Разработчики:

Агаркова О.В.- преподаватель ГПОУ ЯО Переславский колледж им. А. Невского
Малыгина С.Ю., зав.кафедрой ИС, преподаватель ГПОУ ЯО Переславский колледж им. А. Невского
Шендрик А.Е., руководитель центра ИТ и ЭОР

Утверждаю
Заместитель директора по УПР

Рассмотрена на заседании кафедры ИС

Протокол №__от_____201_г. Зав. кафедрой_____С.Ю. Малыгина

_____Н.К.Чернышова

«____»_____201_г.

**Содержание**

# 1.ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

## 1.1. Область применения программы

Рабочая программа учебной практики является составной частью программы подготовки специалистов среднего звена (ППССЗ, обеспечивающей реализацию Федерального государственного образовательного стандарта среднего профессионального образования (ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основных видов профессиональной деятельности (ВПД):

- Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
- Защита информации в автоматизированных системах программными и программно-аппаратными средствами
- Защита информации техническими средствами
- Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин.

Рабочая программа учебной практики может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке работников в области защиты информации.

## 1.2. Цели и задачи учебной практики:

Формирование у обучающихся умений, приобретение первоначального практического опыта в рамках профессиональных модулей ППССЗ СПО по основным видам профессиональной деятельности, необходимых для последующего освоения ими общих и профессиональных компетенций по избранной специальности.

С целью овладения указанными видами профессиональной деятельности обучающийся в ходе учебной практики должен:

**Вид профессиональной деятельности (ВПД): <u>Эксплуатация автоматизированных (информационных) систем в защищенном исполнении</u>.**

**иметь первоначальный практический опыт в:**

- эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;

- администрировании автоматизированных систем в защищенном исполнении;
- установке компонентов систем защиты информации автоматизированных информационных систем.

**уметь:**

- обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;
- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;
- организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;
- настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.

**Вид профессиональной деятельности (ВПД): <u>Защита информации в автоматизированных системах программными и программно-аппаратными средствами</u>**

**иметь первоначальный практический опыт в:**

- установке и настройке программных средств защиты информации;
- тестировании функций, диагностики, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;
- учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

**уметь:**

- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
- использовать типовые программные криптографические средства, в том числе электронную подпись;
- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
- 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.

**Вид профессиональной деятельности (ВПД): Защита информации техническими средствами**

**иметь первоначальный практический опыт в:**

- выявлении технических каналов утечки информации;
- применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;
- проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
- проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

**уметь:**

- применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
- применять технические средства для криптографической защиты информации конфиденциального характера;
- применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;
- применять инженерно-технические средства физической защиты объектов информатизации.

**Вид профессиональной деятельности (ВПД): Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин**

**иметь первоначальный практический опыт:**

- выполнения требований техники безопасности при работе с вычислительной техникой;
- организации рабочего места оператора электронно-вычислительных и вычислительных машин;
- подготовки оборудования компьютерной системы к работе;
- инсталляции, настройки и обслуживания программного обеспечения компьютерной системы;
- управления файлами;
- применения офисного программного обеспечения в соответствии с прикладной задачей;
- использования ресурсов локальной вычислительной сети;
- использования ресурсов, технологий и сервисов Интернет;
- применения средств защиты информации в компьютерной системе.

**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

**1.3. Количество часов на освоение рабочей программы учебной практики:**
Всего 450 часов, в том числе:
В рамках освоения ПМ.01 - 3 недели, 108 часов.
В рамках освоения ПМ.02 - 4 недели, 144 часа.
В рамках освоения ПМ.03 – 3,5 недели 126 часов.
В рамках освоения ПМ.04 - 2 недели, 72 часа.

## 2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Результатами освоения рабочей программы учебной практики являются: сформированные у обучающихся умения, приобретенный первоначальный практический опыт в рамках профессиональных модулей ППССЗ СПО по основным видам профессиональной деятельности (ВПД): *эксплуатация автоматизированных (информационных) систем в защищенном исполнении; защита информации в автоматизированных системах программными и программно-аппаратными средствами; защита информации техническими средствами, выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин,* необходимые для последующего освоения ими профессиональных (ПК) и общих (ОК) компетенций по избранной специальности.

| ВПД | Наименование результата освоения практики |
|---|---|
| Эксплуатация автоматизированных (информационных) систем в защищенном исполнении | **Первоначальный практический опыт:**<br>– эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;<br>– администрирования автоматизированных систем в защищенном исполнении;<br>– установки компонентов систем защиты информации автоматизированных информационных систем.<br>**Умения:**<br>– обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;<br>– производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;<br>– организовывать, конфигурировать, производить |

| | |
|---|---|
| | монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;<br>– настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам. |
| Защита информации в автоматизированных системах программными и программно-аппаратными средствами | **Первоначальный практический опыт:**<br>– установки и настройки программных средств защиты информации;<br>– тестирования функций, диагностики, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;<br>– учета, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности.<br>**Умения:**<br>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;<br>– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;<br>– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;<br>– использовать типовые программные криптографические средства, в том числе электронную подпись;<br>– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;<br>– 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. |
| Защита информации техническими средствами | **Первоначальный практический опыт в:**<br>– выявлении технических каналов утечки информации;<br>– применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;<br>– проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;<br>– проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.<br>**Умения:**<br>– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;<br>– применять технические средства для криптографической защиты информации конфиденциального характера;<br>– применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;<br>– применять инженерно-технические средства физической защиты объектов информатизации. |
| Выполнение работ по профессии | **Первоначальный практический опыт:**<br>– выполнения требований техники безопасности при |

| | |
|---|---|
| рабочего 16199 Оператор электронно-вычислительных и вычислительных машин | работе с вычислительной техникой;<br>− организации рабочего места оператора электронно-вычислительных и вычислительных машин;<br>− подготовки оборудования компьютерной системы к работе;<br>− инсталляции, настройки и обслуживания программного обеспечения компьютерной системы;<br>− управления файлами;<br>− применения офисного программного обеспечения в соответствии с прикладной задачей;<br>− использования ресурсов локальной вычислительной сети;<br>– использования ресурсов, технологий и сервисов Интернет;<br>– применения средств защиты информации в компьютерной системе.<br>**Умения:**<br>– выполнять требования техники безопасности при работе с вычислительной техникой;<br>– производить подключение блоков персонального компьютера и периферийных устройств;<br>– производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники;<br>– диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники;<br>– выполнять инсталляцию системного и прикладного программного обеспечения;<br>– создавать и управлять содержимым документов с помощью текстовых процессоров;<br>– создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц;<br>– создавать и управлять содержимым презентаций с помощью редакторов презентаций;<br>– использовать мультимедиа проектор для демонстрации презентаций;<br>– вводить, редактировать и удалять записи в базе данных;<br>– эффективно пользоваться запросами базы данных;<br>– создавать и редактировать графические объекты с помощью программ для обработки растровой и |

| | |
|---|---|
| | векторной графики;<br>– производить сканирование документов и их распознавание;<br>– производить распечатку, копирование и тиражирование документов на принтере и других устройствах;<br>– управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете;<br>– осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера;<br>– осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов;<br>– осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ;<br>– осуществлять резервное копирование и восстановление данных |

## 3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

### 3.1. Тематический план учебной практики

| Код и наименование профессионального модуля | Наименование тем учебной практики | Количество часов по темам |
|---|---|---|
| **ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении** | Тема 1.1 Введение в платформу SQL Server Установка SQL Server 2016 | 8 |
| | Тема 1.2. Работа с базами данных и механизмом хранения | 7 |
| | Тема 1.3. Резервирование баз данных | 7 |
| | Тема 1.4 Восстановление баз данных | 7 |
| | Тема 1.5 Импорт и экспорт данных | 7 |
| | Тема 1.6 Трассировка событий на сервере | 8 |
| | Тема 1.7 Управление защитой данных | 7 |
| | Тема 1.8 Шифрование и аудит | 7 |
| | Тема 1.9 Регламентные задачи | 7 |
| | Тема 1.10 Автоматизация управления сервером Устранение типовых проблем | 7 |
| | Тема 2.1 Монтаж кабельной сети и оборудования локальных сетей различных топологий | 3 |
| | Тема 2.2 Настройка сетевых протоколов серверов и рабочих станций | 2 |
| | Тема 2.3 Эксплуатация и обслуживание сетевого оборудования | 3 |
| | Тема 2.4 Работа с системой регистрации и авторизации пользователей сети | 3 |

| | | |
|---|---|---|
| | | |
| | Тема 2.5 Системное администрирование локальных сетей | 4 |
| | Тема 2.6 Установка и настройка подключения к Интернету с помощью различных технологий и специализированного оборудования | 7 |
| | Тема 2.7 Выбор подключения и тарифного плана у провайдера доступа в Интернет | 2 |
| | Тема 2.8 Установка специализированных программ и драйверов. Настройка параметров подключения к Интернету | 2 |
| | Тема 2.9 Управление и учет входящего и исходящего трафика сети | 3 |
| | Тема 2.10 Установка и настройка программного обеспечения серверов Интернета. Обеспечение резервного копирования данных. | 2 |
| | Тема 2.11 Защита компьютерных сетей от несанкционированного доступа. Мероприятия по защите персональных данных | 2 |
| | Тема 2.12 Применение специализированных средств для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами. | 1 |
| | Дифференцированный зачет | 2 |
| | **Всего часов:** | **108** |
| **ПМ.02 Защита информации в автоматизированных** | Тема 1 Управление локальным пользователями и группами в ОС Windows | 8 |

| | | |
|---|---|---|
| **системах программными и программно-аппаратными средствами** | Тема 2. Знакомство с файловой системой NTFS | 7 |
| | Тема 3. Механизм разрешений в Windows | 7 |
| | Тема 4. Совместное использование сетевых ресурсов | 7 |
| | Тема 5. Использование шифрования в NTFS | 7 |
| | Тема 6. Использование службы каталогов Active Directory | 8 |
| | Тема 7. Использование групповых политик и шаблонов безопасности | 7 |
| | Тема 8. Резервное копирование и отказоустойчивые системы | 7 |
| | Тема 9. Мониторинг событий и аудит. Мониторинг производительности | 7 |
| | Тема 10. Использование инфраструктуры открытых ключей | 7 |
| | Тема 11. Защита информации при передаче в сети | 8 |
| | Тема 12. Антивирусная защита | 7 |
| | Тема 13. Защита информации от несанкционированного доступа | 14 |
| | Тема 14. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи | 7 |
| | Тема 15. Выполнение профессиональных заданий | 34 |
| | Дифференцированный зачет | 2 |
| | **Всего часов:** | **144** |

| | | |
|---|---|---|
| **ПМ.03 Защита информации техническими средствами** | Тема 1.1 Действие электрического тока на организм человека. | 2 |
| | Тема 1.2 Оказание первой помощи пострадавшему | 2 |
| | Тема 1.3 Требования безопасности при выполнении работ | 2 |
| | Тема 1.4 Контрольное занятие по теме Электробезопасность | 2 |
| | Тема 2.1 Цифровой мультиметр | 2 |
| | Тема 2.2 Проведение измерений цифровым мультиметром. | 5 |
| | Тема 2.3 Стрелочные измерительные приборы (мультиметр). | 4 |
| | Тема 2.4 Стрелочные измерительные приборы (мегаомметр). | 3 |
| | Тема 3.1 Электрический паяльник | 2 |
| | Тема 3.2 Порядок подготовки паяльника к работе | 1 |
| | Тема 3.3 Подготовка паяльника к работе. | 2 |
| | Тема 3.4 Порядок лужения проводов | 2 |
| | Тема 3.5. Лужение проводов | 3 |
| | Тема 3.6 Порядок пайки проводных соединений | 1 |
| | Тема 3.7 Пайка проводных соединений | 3 |
| | Тема 3.8 Пайка разъемов | 5 |
| | Тема 3.9 Изготовление клемм | 3 |
| | Тема 4.1 Радиоэлементная база | 4 |
| | Тема 4.2 Полупроводниковые радиоэлементы | 3 |
| | Тема 4.3 Пайка пассивных и активных элементов | 7 |
| | Тема 4.4 Блоки питания | 7 |
| | Тема 4.5 Генераторы | 7 |
| | Тема 4.6 Мультивибраторы | 7 |
| | Тема 4.7 Усилители низкой частоты (УНЧ) | 7 |

| | | |
|---|---|---|
| | Тема 4.8. Реле, электронные ключи | 4 |
| | Тема 5.1 Прибор SEL SP-77/2 | 2 |
| | Тема 5.2 Контрольное устройство Тест-031 | 2 |
| | Тема 5.3 Прибор SEL SP-17/D | 3 |
| | Тема 5.4 Прибор SEL SP-55 | 3 |
| | Тема 5.5 Работа с прибором SEL SP-55 | 4 |
| | Тема 5.6 Блокираторы сотовых телефонов | 7 |
| | Тема 5.7 Многофункциональный поисковый прибор ST-032 «Пиранья» | 3 |
| | Тема 5.8 Работа с прибором ST-032 «Пиранья» | 4 |
| | Тема 5.9 GSM датчиков Pir Mr Alert и N9 | 2 |
| | Тема 5.10 Детектор жучков и скрытых камер CC308+ | 2 |
| | Тема 5.11 Работа по выявлению жучков, радиомаяков и скрытых камер и их поиск | 2 |
| | Дифференцированный зачет | 2 |
| | **Всего часов:** | **126** |
| **ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих** | Тема 1.1 Работа с устройствами компьютерной системы | 8 |
| | Тема 1.2 Работа с программным обеспечением компьютерной системы | 7 |
| | Тема 1.3 Диагностика неисправностей системы, ведение документации | 7 |
| | Тема 2.1 Работа в текстовом процессоре | 7 |
| | Тема 2.2 Работа в редакторе электронных таблиц | 7 |
| | Тема 2.3 Работа в программе подготовки и просмотра презентаций | 7 |
| | Тема 2.4 Работа в системе управления базами данных | 7 |
| | Тема 2.5 Работа в графических редакторах | 8 |

| | | |
|---|---|---|
| | Тема 3.1 Работа с ресурсами Интернета | 7 |
| | Тема 4.1 Защита информации при работе с офисными приложениями | 5 |
| | Дифференцированный зачет | 2 |
| | **Всего часов:** | **72** |
| | **Итого:** | **450** |

## 3.2. Содержание учебной практики

| Код и наименование профессиональных модулей и тем учебной практики | Содержание учебных занятий | Количество часов по темам |
|---|---|---|
| **ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении** | | **108** |
| Тема 1.1 Введение в платформу SQL Server Установка SQL Server 2016 | 1. Платформа SQL Server<br>2. Инструменты для администрирования<br>3. Службы и конфигурация<br>4. Подготовка к установке<br>5. Установка и настройка. | 8 |
| Тема 1.2. Работа с базами данных и механизмом хранения | 1. Создание базы данных<br>2. Файлы и файловые группы. Перемещение файлов. Расширение буферного пула. | 7 |
| Тема 1.3. Резервирование баз данных | 1. Модели восстановления<br>2. Стратегии резервного копирования<br>3. Журналирование транзакций<br>4. Планирование резервного копирования<br>5. Резервирование баз и журналов | 7 |
| Тема 1.4 Восстановление баз данных | 1. Процесс восстановления<br>2. Восстановление баз данных<br>3. Дополнительные возможности при восстановлении<br>4. Восстановление на заданный момент времени | 7 |

| | | |
|---|---|---|
| Тема 1.5 Импорт и экспорт данных | 1. Перемещение данных<br>2. Импорт и экспорт табличных данных<br>3. Массовый импорт данных | 7 |
| Тема 1.6 Трассировка событий на сервере | 1. Перехват событий при помощи SQL Server Profiler<br>2. Настройки трассировки | 8 |
| Тема 1.7 Управление защитой данных | 1. Механизмы защиты данных<br>2. Управление защитой сервера<br>3. Пользователи базы данных<br>4. Настройка разрешений | 7 |
| Тема 1.8 Шифрование и аудит | 1. Отслеживание доступа к данным<br>2. Использование аудита<br>3. Управление аудитом<br>4. Защита данных при помощи шифрования | 7 |
| Тема 1.9 Регламентные задачи | 1. Целостность базы данных<br>2. Обслуживание индексов<br>3. Автоматизация регламентных задач | 7 |
| Тема 1.10 Автоматизация управления сервером. Устранение типовых проблем | 1. Автоматизация управления сервером<br>2. Работа с агентом<br>3. Управление задачами<br>4. Типовые проблемы и сбои сервера<br>5. Типовые проблемы при подключении | 7 |
| Тема 2.1 Монтаж кабельной сети и оборудования локальных сетей различных топологий. | 1. Обжим коаксиального кабеля. Маркировка коаксиального кабеля. Диагностика.<br>2. Монтаж обжимных разъемов. Маркировка кабеля «витая пара». Диагностика.<br>3. Монтаж соединителей и разделка оптоволоконного кабеля. Маркировка оптоволоконного кабеля. Сращивание кабеля. Диагностика. | 3 |
| Тема 2.2 Настройка сетевых протоколов серверов и рабочих станций. | 1. Определение сетевых возможностей Windows при подключении к сети.<br>2. Определение конфигурации локальной сети.<br>3. Настройка Интернет-центра для подключения к Интернету по | 2 |

| | | |
|---|---|---|
| | протоколу PPPoE.<br>4.Настройка Интернет-центра для подключения к Интернету по протоколу PPTP.<br>5. Настройка Интернет-центра для подключения к Интернету по протоколу L2TP.<br>6. Настойка Интернет-центра для подключения к Интернету с использованием статического (постоянного) внешнего IP-адреса.<br>7. Настройка Интернет-центра статических маршрутов. | |
| Тема 2.3 Эксплуатация и обслуживание сетевого оборудования. | 1. Настройка платы сетевого адаптера.<br>2. Диагностика платы сетевого адаптера.<br>3. Установка и настройка сетевого принтера.<br>4. Поиск и устранение проблем сетевого принтера.<br>5. Подключение и настройка модема.<br>6. Диагностика модема. | 3 |
| Тема 2.4 Работа с системой регистрации и авторизации пользователей сети. | 1.Авторизация пользователей сети через Active Directory посредством контроллера Windows домена.<br>2. Авторизация пользователей по IP адресу.<br>3. Авторизация пользователей сети посредством туннелей через VPN подключение к серверу контроля корпоративного Интернет доступа (например PPTP или L2TP).<br>4. Авторизация пользователей сети по протоколу PPPoE. | 3 |
| Тема 2.5 Системное администрирование локальных сетей. | 1.Учет компьютеров в сети предприятия, просмотр конфигурации удаленных компьютеров и списки установленных программ по сети, отслеживание изменения конфигурации и ПО с помощью программы для инвентаризации и учета установленного программного и аппаратного обеспечения на | 4 |

| | | |
|---|---|---|
| | компьютерах в локальных сетях «Инвентаризация компьютеров».<br>2. Визуальное наблюдение текущего состояния сети в любой момент времени с помощью программы мониторинга серверов и компьютеров в сети 10-Strike LANState.<br>3.Контроль работоспособности сети и неполадок с помощью программы Мониторинга Сети. | |
| Тема 2.6 Установка и настройка подключения к Интернету с помощью различных технологий и специализированного оборудования. | 1. Подключение по коммутируемой телефонной линии с помощью модема. Работа с утилитой подключения.<br>2. Подключение ADSL-доступа с применением телефонной линии.<br>3. Организация подключение «классических» выделенных каналов на основе медной пары городской телефонной сети, оптоволоконного канала или радиолинии.<br>4. Подключение к сети Интернет с использованием роутера (точки доступа).<br>5. Подключение к Интернет с помощью выделенного канала.<br>6. Подключение к Интернет с применением спутниковой антенны.<br>7. Создание локальной сети с использованием роутера (точки доступа). | 7 |
| Тема 2.7 Выбор подключения и тарифного плана у провайдера доступа в Интернет. | 1. Выбор технологии подключения к сети Интернет.<br>2. Выбор тарифного плана у провайдера доступа в Интернет. | 2 |
| Тема 2.8 Установка специализированных программ и драйверов. Настройка параметров подключения к Интернету. | 1. Работа с оптимизатором подключений.<br>2. Работа с утилитой ведения статистики.<br>3. Настройка и приемы работы с браузерами Internet Explorer, FireFox, Google Chrome, Opera. | 2 |

| | | |
|---|---|---|
| Тема 2.9 Управление и учет входящего и исходящего трафика сети. | 1. Контроль за объемами скачиваемых данных и скоростью передачи информации в сети с помощью программы Учет Трафика.<br>2. Ограничение прав для пользователей по: использованию рабочей станции или сервера; - времени; степени использования ресурсов. | 3 |
| Тема 2.10 Установка и настройка программного обеспечения серверов Интернета. Обеспечение резервного копирования данных. | 1. Работа с утилитой удаленного администрирования через Интернет.<br>2. Настройка и приемы работы с прокси-сервером.<br>3. Резервное сохранение и восстановление данных. Выбор метода архивации.<br>4. Сохранение резервных копий с помощью специализированных программ. | 2 |
| Тема 2.11 Защита компьютерных сетей от несанкционированного доступа. Мероприятия по защите персональных данных | 1. Работа со специальным программным обеспечением по защите ПК.<br>2. Защита документов в Ms Word.<br>3. Защита книг Ms Excel.<br>4. Настройка защищенного сетевого обеспечения.<br>5. Настройка сканера безопасности операционных систем.<br>6. Парольная защита баз данных Ms Access.<br>7. Создание защищенной базы данных Ms Access.<br>8. Администрирование базы данных. | 2 |
| Тема 2.12 Применение специализированных средств для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами. | 1. Защита антивирусной программы NOD32 Antivirus.<br>2. Использование антивирусной программы Doctor Web.<br>3. Использование антивирусной программы Антивирус Касперского.<br>4. Использование антивирусной программы Norton Antivirus.<br>5. Использование антивирусной программы McAfee VirusScan. | 1 |

| | | |
|---|---|---|
| | 6. Использование антивирусной программы Panda Antivirus. | |
| | Дифференцированный зачет | 2 |
| **ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами** | | **144** |
| Тема 1 Управление локальным пользователями и группами в ОС Windows | 1. Понятие учетной записи пользователя<br>2. Группы пользователей<br>3. Администрирование учетных записей пользователей групп с помощью графического интерфейса<br>4. Использование командной строки для администрирования учетных записей пользователей и групп<br>5. использование командных файлов | 8 |
| Тема 2. Знакомство с файловой системой NTFS | 1. Файловые системы в ОС Windows<br>2. Основные возможности ФС NTFS<br>3. Использование механизма разрешений на доступ к объектам ФС<br>4. Управление разрешениями на объекты ФС<br>5. Владельцы объектов ФС, смена владельца<br>6. Использование командной строки для управления доступом к объектам ФС | 7 |
| Тема 3. Механизм разрешений в Windows | 1. Действующие разрешения<br>2. Встроенные участники системы безопасности (Неявные группы)<br>3. Идентификаторы безопасности и маркеры доступа<br>4. Дескрипторы безопасности<br>5. Контроль учетных записей | 7 |

| | | |
|---|---|---|
| Тема 4. Совместное использование сетевых ресурсов | 1. Общие ресурсы<br>2. Домены, рабочие группы и домашние группы<br>3. Управление общим доступом к ресурсу<br>4. Использование общих ресурсов в сети<br>5. Определение суммарных разрешений на сетевой ресурс<br>6. Специальные сетевые ресурсы | 7 |
| Тема 5. Использование шифрования в NTFS | 1. Шифрующая файловая система (EFS)<br>2. Принцип работы EFS<br>3. Использование графического интерфейса для взаимодействия с EFS<br>4. Взаимодействие с EFS из командной строки.<br>5. Агенты восстановления EFS<br>6. Средство шифрования BitLocker<br>7. Использование BitLocker | 7 |
| Тема 6 Использование службы каталогов Active Directory | 1. Назначение службы каталогов<br>2. Система безопасности<br>3. Kerberos в службе каталогов | 8 |
| Тема 7 Использование групповых политик и шаблонов безопасности | 1. Групповые политики<br>2. Объекты групповой политики<br>3. Настройка объектов групповой политики<br>4. Настройка параметров безопасности | 7 |
| Тема 8 Резервное копирование и отказоустойчивые системы | 1. Резервное копирование данных<br>2. Стратегии резервного копирования<br>3. Восстановление данных<br>4. Отказоустойчивые дисковые системы<br>5. Настройка и использование отказоустойчивой дисковой системы. Механизмы защиты данных<br>6. Управление защитой сервера<br>7. Пользователи базы данных | 7 |

| | | |
|---|---|---|
| | 8. Настройка разрешений | |
| Тема 9 Мониторинг событий и аудит. Мониторинг производительности | 1. Просмотр событий<br>2. Работа с журналами<br>3. Настройка аудита<br>4. Аудит доступа к объектам<br>5. Использование диспетчера задач<br>6. Мониторинг производительности | 7 |
| Тема 10 Использование инфраструктуры открытых ключей | 1. Сертификаты<br>2. Инфраструктура открытых ключей<br>3. Использование PKI в ОС Windows<br>4. использование смарткарт и usb-токенов для хранения сертификатов<br>5. использование eToken | 7 |
| Тема 11 Защита информации при передаче в сети | 1. Модель ISO/OSI<br>2. Межсетевое взаимодействие средствами TCP/IP<br>3. Сетевой анализатор<br>4. Настройка использования протокола HTTPS на срвере IIS<br>5. Технология IPSec<br>6. Брандмауер Windows | 8 |
| Тема 12 Антивирусная защита | 1. Компьютерные вирусы<br>2. Признаки заражения вирусами<br>3. Антивирусные программы | 7 |
| Тема 13 Защита информации от несанкционированного доступа | 1. Средства доверенной загрузки<br>2. Программно-аппаратный ключ «Соболь» | 7 |
| | 1. Необходимость использования СЗИ от НСД<br>2. СЗИ от НСД SecretNet<br>3. Защитные механизмы SecretNet<br>4. Защита входа в систему<br>5. Замкнутая программная среда | 7 |

| | | |
|---|---|---|
| | 6. Контроль целостности<br>7. Разграничение доступа устройствам | |
| | Тема 14. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи | 7 |
| | Тема 15. Выполнение профессиональных заданий | 34 |
| | Дифференцированный зачёт | 2 |
| **ПМ.03 Защита информации техническими средствами** | | **126** |
| Тема 1.1 Действие электрического тока на организм человека. | 1. Электрический ток (ЭТ).<br>2. Факторы, влияющие на исход поражения человека ЭТ.<br>3. Виды поражения человека электрическим током.<br>4. Классификация помещений по степени опасности поражения ЭТ. | 2 |
| Тема 1.2 Оказание первой помощи пострадавшему | 1. Порядок освобождения пострадавшего от действия ЭТ.<br>2. Оценка состояния пострадавшего от действия ЭТ.<br>3. Выполнение искусственного дыхания.<br>4. Выполнение непрямого массажа сердца.<br>5. Оказание первой помощи при ожогах.<br>6. Оказание первой помощи при отравлениях ЯТЖ. | 2 |
| Тема 1.3 Требования безопасности при выполнении работ | 1. Технические мероприятия, обеспечивающие безопасность работ на электроустановках.<br>2. Защитные средства. Электроинструмент.<br>3. Требования безопасности при | 2 |

| | | |
|---|---|---|
| | работе с электроинструментом.<br>4. Требования безопасности при работе на высоте. | |
| Тема 1.4 Контрольное занятие по теме Электробезопасность | 1. Самостоятельная подготовка.<br>2. Контрольная работа (письменная).<br>3. Инструктаж по требованиям безопасности (ТБ) на рабочем месте. Заполнение Журнала инструктажей по ТБ. Допуск к работе. | 2 |
| Тема 2.1 Цифровой мультиметр | 1. Назначение, состав и общее устройство цифрового мультиметра.<br>2. Подготовка мультиметра к работе. Дополнительные функции.<br>3. Порядок проведения измерений мультиметром. | 2 |
| Тема 2.2 Проведение измерений цифровым мультиметром. | 1. Измерение постоянного напряжения элементов питания и напражения зарядного устройства.<br>2. Измерение переменного напряжения бытовой сети.<br>3. Измерение постоянного тока в замкнутой цепи.<br>4.Измерение электрического сопротивления, прозвонка кабеля. | 5 |
| Тема 2.3 Стрелочные измерительные приборы (мультиметр). | 1. Назначение, состав и общее устройство стрелочного мультиметра.<br>2. Шкала. Символы и обозначения шкалы, определяющие работу прибора. Порядок определения измеряемой величины по шкале.<br>3. Измерение физических величин стрелочным мультиметром. | 4 |
| Тема 2.4 Стрелочные измерительные приборы (мегаомметр). | 1. Назначение и порядок работы с мегаомметром.<br>2. Измерение сопротивления изоляции основных средств защиты и электроинструмента мегаомметром. | 3 |
| Тема 3.1 Электрический паяльник | 1. Назначение электрического паяльника.<br>2. Классификация паяльников.<br>3. Общее устройство электрического паяльника.<br>4. Припой. Назначение и его | 2 |

| | | |
|---|---|---|
| | разновидности.<br>5. Флюсы. Применение флюсов для пайки и лужения. | |
| Тема 3.2 Порядок подготовки паяльника к работе | 1. Выбор паяльника для различных работ.<br>2. Проверка состояния паяльника и его работоспособности.<br>3. Подготовка жала паяльника к работе. | 1 |
| Тема 3.3 Подготовка паяльника к работе. | 1. Подготовка жала паяльника, ковка, зачистка.<br>2. Обработка жала канифолью, припоем, лужение.<br>3. Лужение и пайка проводов. | 2 |
| Тема 3.4 Порядок лужения проводов | 1. Основные правила при лужении проводов.<br>2. Подготовка провода к лужению.<br>3. Порядок лужения проводов. | 2 |
| Тема 3.5. Лужение проводов | 1. Выбор проводника.<br>2. Отчистка провода от изоляции.<br>3. Лужение проводов. | 3 |
| Тема 3.6 Порядок пайки проводных соединений | 1. Основные правила при пайки двух и более проводников.<br>2. Порядок подготовки проводников к пайке. Классификация скруток проводников.<br>3. Порядок пайки проводных соединений. | 1 |
| Тема 3.7 Пайка проводных соединений | 1. Подготовка проводников к пайке. Выбор скрутки проводников.<br>2. Пайка проводных соединений. | 3 |
| Тема 3.8 Пайка разъемов | 1. Подготовка разъема и проводника к пайке.<br>2. Пайка разъемов.<br>3. Использование кембриков и термоусадки для изоляции оголенной части провода. | 5 |
| Тема 3.9 Изготовление клемм | 1. Пайка неизолированных кольцевых и ножевых клемм.<br>2. Изготовление клемм из проводов.<br>3. Обжим проводов трубчатыми | 3 |

| | | |
|---|---|---|
| | наконечниками с использованием обжимных клещей. | |
| Тема 4.1 Радиоэлементная база | 1. Классификация радиоэлементов.<br>2. Резисторы. Условное обозначение.<br>3. Конденсаторы. Условное обозначение.<br>4. Катушки индуктивности. Условное обозначение.<br>5. Трансформаторы. Условное обозначение.<br>6. Прозвонка и измерение сопротивления резисторов, катушек индуктивности, трансформаторов, проверка конденсаторов. | 4 |
| Тема 4.2 Полупроводниковые радиоэлементы | 1. Диоды. Условное обозначение.<br>2. Транзисторы. Условное обозначение.<br>3. Интегральные микросхемы. Условное обозначение.<br>4. Чтение принципиальных электрических и монтажных схем.<br>5. Особенности пайки радиоэлементов.<br>6. Прозвонка диодов и транзисторов мультиметром. | 3 |
| Тема 4.3 Пайка пассивных и активных элементов | 1. Подготовка и пайка резисторов, конденсаторов, катушек индуктивности, трансформаторов.<br>2. Подготовка и пайка диодов, изготовление диодных мостов.<br>3. Подготовка и пайка транзисторов, микросхем.<br>4. Порядок проверки качества пайки.<br>5. Порядок изготовления монтажных плат из текстолита. | 7 |
| Тема 4.4 Блоки питания | 1. Общие понятия о блоках питания. Принцип их построения.<br>2. Проектирование и составление блока питания.<br>3. Сборка и пайка блока питания. | 7 |

| | | |
|---|---|---|
| Тема 4.5 Генераторы | 1. Общие понятия о генераторах. Принцип их построения.<br>2. Проектирование и составление простейшего генератора.<br>3. Сборка и пайка простейшего генератора. | 7 |
| Тема 4.6 Мультивибраторы | 1. Общие понятия о мультивибраторах.<br>2. Проектирование и составление мультивибратора.<br>3. Сборка и пайка мультивибратора. | 7 |
| Тема 4.7 Усилители низкой частоты (УНЧ) | 1. Общие понятия о УНЧ. Принцип их построения.<br>2. Проектирование и составление простейшего УНЧ.<br>3. Сборка и пайка простейшего УНЧ. | 7 |
| Тема 4.8. Реле, электронные ключи | 1. Общие понятия о реле и электронных ключах.<br>2. Проектирование и составление устройств с использованием реле.<br>3. Сборка и пайка устройств с реле и электронными ключами. | 4 |
| Тема 5.1 Прибор SEL SP-77/2 | 1. Цели и задачи практики. Порядок выполнения работ. Инструктаж по технике безопасности.<br>2. Назначение и технические характеристики прибора.<br>3. Порядок работы с прибором. | 2 |
| Тема 5.2 Контрольное устройство Тест-031 | 1. Назначение и технические характеристики прибора.<br>2. Порядок работы с прибором. | 2 |
| Тема 5.3 Прибор SEL SP-17/D | 1. Назначение и технические характеристики прибора.<br>2. Защита телефонных линий прибором SEL SP-17/D. | 3 |
| Тема 5.4 Прибор SEL SP-55 | 1. Назначение и технические характеристики прибора<br>2. Порядок защиты от утечек информации по акустическому каналу. | 3 |
| Тема 5.5 Работа с прибором SEL SP-55 | 1. Порядок работы с прибором.<br>2. Монтаж излучателей. | 4 |

| | | |
|---|---|---|
| | | |
| Тема 5.6 Блокираторы сотовых телефонов | 1. Назначение, состав и технические характеристики «Бархан-1».<br>2. Назначение, состав и технические характеристики прибора<br>3. Порядок работы с приборами. | 7 |
| Тема 5.7 Многофункциональный поисковый прибор ST-032 «Пиранья» | 1. Назначение прибора и его состав.<br>2. Технические характеристики прибора. | 3 |
| Тема 5.8 Работа с прибором ST-032 «Пиранья» | 1.Порядок работы прибор<br>а с комплектом приданных датчиков.<br>2. Практическая работа с прибором по выявлению каналов утечки. | 4 |
| Тема 5.9 GSM датчиков Pir Mr Alert и N9 | 1. Назначение и технические характеристики приборов.<br>2. Порядок управления и работы с приборами.<br>3. Порядок выбора мест скрытой установки приборов. | 2 |
| Тема 5.10 Детектор жучков и скрытых камер CC308+ | 1. Назначение и технические характеристики прибора.<br>2. Порядок работы с прибором.<br>3. Порядок поиска мест установки закладных устройств. | 2 |
| Тема 5.11 Работа по выявлению жучков, радиомаяков и скрытых камер и их поиск | 1. Закладка жучков, радиомаяков, скрытых камер.<br>2. Выявление жучков, радиомаяков, скрытых камер. | 2 |
| | Дифференцированный зачёт | 2 |
| **ПМ.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных** | | **72** |

| | | |
|---|---|---|
| **машин** | | |
| Тема 1.1<br>Работа с устройствами компьютерной системы | 1. Соблюдение техники безопасности при работе на ЭВМ<br>2. Подключение основных и периферийных устройств компьютера. Подключение кабельной системы персонального компьютера, периферийного устройства<br>3. Освоение профессиональных приемов работы с устройствами ввода<br>4. Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка<br>5. Разборка и сборка системного блока. | 8 |
| Тема 1.2<br>Работа с программным обеспечением компьютерной системы | 1. Установка операционной среды, настройка интерфейса ОС (рабочий стол, безопасность системы, подключение к сети).<br>2. Установка прикладных программ.<br>3. Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете | 7 |
| Тема 1 3<br>Диагностика неисправностей системы, ведение документации | 1. Компьютерная диагностика устройств Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники<br>2. Техническое обслуживание системного блока, устройств ввода. Установка и замена расходных материалов для принтеров, ксерокса, плоттера<br>3. Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ | 7 |
| Тема 2.1<br>Работа в текстовом | 1. Сканирование текстовых документов и их распознавание | 7 |

| | | |
|---|---|---|
| процессоре | 2. Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации, сохранение документов<br>3. Форматирование и редактирование документов в текстовом процессоре.<br>4. Работа с таблицами в текстовом процессоре.<br>5. Работа с диаграммами в текстовом процессоре.<br>6. Работа с графическими объектами в текстовом процессоре.<br>7. Печать документов в текстовом процессоре. | |
| Тема 2.2<br>Работа в редакторе электронных таблиц | 1. Создание и форматирование таблицы в редакторе электронных таблиц<br>2. Вычисление с помощью формул в электронной таблице<br>3. Работа со встроенными функциями в электронной таблице<br>4. Работа со списками в электронной таблице<br>5. Создание форм для ввода данных в таблицы<br>6. Создание и работа с диаграммами и графиками<br>7. Обмен данными между текстовым процессором и электронной таблицей | 7 |
| Тема 2.3<br>Работа в программе подготовки и просмотра презентаций | 1. Построение презентации различными способами<br>2. Обработка объектов слайдов презентации<br>3. Настройка анимации объектов<br>4. Настройка показа и демонстрация результатов работы средствами мультимедиа | 7 |
| Тема 2.4<br>Работа в системе управления базами данных | 1. Ввод данных в таблицы базы данных<br>2. Создание простых запросов без параметров и с параметрами. Создание отчетов. | 7 |
| Тема 2.5 | 1. Рисование объектов средствами | 8 |

| | | |
|---|---|---|
| Работа в графических редакторах | графического редактора.<br>2 Работа с заливками и контурами в программе векторной графики.<br>3. Работа с текстом в программе векторной графики.<br>4. Работа с эффектами программе векторной графики.<br>5. Вставка и редактирование готового изображения с использованием программ растровой графики.<br>6. Работа с цветом с использованием программ растрой графики.<br>7. Работа со слоями с использованием программ растрой графики.<br>8. Работа со спецэффектами с использованием программ растровой графики. | |
| Тема 3.1<br>Работа с ресурсами Интернета | 1. Создание и обмен письмами электронной почты.<br>2. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера.<br>3. Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов.<br>4. Пересылка и публикация файлов данных в Интернете. | 7 |
| Тема 4.1<br>Защита информации при работе с офисными приложениями | 1. Использование штатных средств защиты операционной системы и прикладных программ.<br>2. Применение парольной защиты.<br>3. Установка антивирусных программ, их настройка. Обновление базы.<br>4. Выполнение архивирования данных.<br>5. Выполнение резервного копирования и восстановления данных | 5 |
| | Дифференцированный зачёт | 2 |
| | **Итого:** | **450** |

# 4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

## 4.1. Требования к минимальному материально-техническому обеспечению

*ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении*

Реализация рабочей программы учебной практики предполагает наличие учебного кабинета, лабораторий информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации.

Оборудование учебного кабинета и рабочих мест кабинета:

- рабочее место преподавателя;
- посадочные места для обучающихся;
- аудиовизуальный комплекс;
- комплект обучающего материала (комплект презентаций).

Оборудование лаборатории и рабочих мест лаборатории информационных технологий, программирования и баз данных:

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

Оборудование лаборатории и рабочих мест лаборатории сетей и систем передачи информации:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- стенды сетей передачи данных;
- структурированная кабельная система;
- эмулятор (эмуляторы) активного сетевого оборудования;
- программное обеспечение сетевого оборудования.

Оборудование лаборатории и рабочих мест лаборатории программных и программно-аппаратных средств защиты информации:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- антивирусный программный комплекс;
- программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности.

*ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами*

Реализация программы предполагает наличие учебных кабинетов – лекционные аудитории с мультимедийным оборудованием; лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест - 30, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.

Оборудование лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности» и рабочих мест лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами;
- лабораторные учебные макеты;
- рабочее место преподавателя;
- учебно-методическое обеспечение модуля;
- интерактивная доска, комплект презентаций;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, 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.

*ПМ.03 Защита информации техническими средствами*

лекционные аудитории с мультимедийным оборудованием; лаборатория «Технических средств защиты информации».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест – не менее 30, рабочее место преподавателя, проектор, персональный компьютер, интерактивная доска, комплект презентаций.

Оборудование лаборатории «Технических средств защиты информации» и рабочих мест лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами;
- лабораторные учебные макеты;
- аппаратные средства аутентификации пользователя;
- средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок;
- средства измерения параметров физических полей;
- стенд физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов;
- рабочее место преподавателя;
- учебно-методическое обеспечение модуля;
- интерактивная доска, комплект презентаций.

*ПМ.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин*

Реализация программы учебной практики предполагает наличие лаборатории информационных технологий.

Оборудование лаборатории информационных технологий:

- Компьютеры, объединенные в локальную вычислительную сеть, проектор, экран, акустическая система.
- Программное обеспечение: (операционные системы, пакет прикладных программ, графические редакторы, справочная правовая система, браузер, антивирусная программа)
- Учебно-наглядные пособия: схемы, таблицы, учебные презентации
- Раздаточный дидактический материал: учебные карточки с заданиями, дидактический материал для выполнения практических работ.

## 4.2. Информационное обеспечение учебной практики

Основные источники (ОИ)


1. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2017. – 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. – 2016
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, 2018.- 248 с.
5. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2016.
6. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2017.
7. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 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, 2016. – 417 с.
9. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2017. – 416 с.
10. Киселев С.В. Оператор ЭВМ: учеб. пособие для студ. учреждений сред. проф. образования /. – 7-е изд., испр. – М.: Издательский центр «Академия», 2014.
11. Коньков, К. А. Устройство и функционирование ОС Windows. Практикум к курсу Операционные системы. /Учебное пособие // К.А. Коньков. М.: Бином, Лаборатория знаний Интуит, 2018.
12. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.:

Издательский центр «Академия», 2016.
13. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 2-е изд.- М.: Горячая линия-Телеком, 2017.
14. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2017
15. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2015.
16. 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.
17. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2016. – 172 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, 2017. – 172 с.
19. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2017.
20. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2018. – 336с
21. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2017.
22. Сидоров В.Д. Аппаратное обеспечение ЭВМ: практикум: уч. пособие для НПО. - М.: Издательский центр Академия, 2018. – 160 с.
23. Сидоров В.Д. Аппаратное обеспечение ЭВМ: учебник для НПО. - М.: Издательский центр Академия, 2016. – 336 с.
24. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2016.
25. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
26. Струмпэ Н.В. Оператор ЭВМ. Практические работы: учеб. пособие для нач. проф. образования / – 6-е изд., стер. – М.: Издательский центр «Академия», 2016.
27. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2017.
28. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2017
29. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2017

## Дополнительные печатные источники (ДИ):

1. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.
2. ГубенковА.А. Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2009. - 88 с.

3. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы – М.: Бином, 2011. – 1024 с.
4. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бином, 2011. – 704 с.
5. Жмакин А. П. Архитектура ЭВМ : учеб. пособие для вузов / А. П. Жмакин. - 2-е изд., перераб. и доп. - СПб. : БХВ-Перербург, 2010. - 352 с.: ил. - (Учебная литература для вузов)
6. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник.-М.: Горячая линия-Телеком., 2008
7. Кофлер М., Linux. Полное руководство – Питер, 2011. – 800 с.
8. Кукушкина М.С. Работа в MS Office 2007. Табличный процессор Excel 2007[Текст]. Лабораторные работы. - Ульяновск: УЛГТУ, 2010.
9. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2008
10. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.- М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2007.- 531 с.
11. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.
12. 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.
13. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб. пос. для студентов СПО – М.: Форум, 2013. – 544 с.
14. 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.
15. Руссинович М., Соломон Д., Внутреннее устройство MicrosoftWindows. Основные подсистемы операционной системы – Питер, 2014. – 672 с.
16. Сафонов, В.О. Основы современных операционных систем: учебное пособие. М.: Бином. Лаборатория знаний, 2014. – 583 с.
17. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008. – 368 с.

Периодические издания:

1. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/
2. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
3. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей.
4. Журналы Защита информации. Инсайд: Информационно-методический журнал

5. Информационная безопасность регионов: Научно-практический журнал

Электронные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Компьютер своими руками. [Электронный ресурс]/ ruslan-m.com - режим доступа: http://ruslan-m.com .
4. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
5. Ремонт настройка и модернизация компьютера. [Электронный ресурс]/ remont-nastroyka-pc.ru - режим доступа: http://www.remont- nastroyka-pc.ru.
6. Российский биометрический портал www.biometrics.ru
7. Сайт журнала Информационная безопасность http://www.itsec.ru –
8. Сайт Научной электронной библиотеки www.elibrary.ru
9. Собираем компьютер своими руками. [Электронный ресурс]/ svkcomp.ru -режим доступа: http://www.svkcomp.ru/.
10. Справочно-правовая система «Гарант» » www.garant.ru
11. Справочно-правовая система «Консультант Плюс» www.consultant.ru
12. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
13. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
14. Федеральный портал «Российское образование www.edu.ru

## 4.3. Общие требования к организации образовательного процесса

Учебная практика проводится в рамках профессиональных модулей (непрерывно):

ПМ.01 на 3,4 курсе, в 6,8 семестрах в течение 3 недель;

ПМ.02 на 3,4 курсе, в 6,8 семестрах в течение 4 недель;

ПМ.03 на 3,4 курсе, в 6,8 семестрах в течение 3,5 недель;

ПМ.04 на 2 курсе, в 4 семестре в течение 2 недель.

Продолжительность учебной практики 36 часов в неделю. Практика завершается дифференцированным зачетом.

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

## 4.4. Кадровое обеспечение образовательного процесса

**Требования к квалификации педагогических кадров, осуществляющих руководство практикой.**

Учебная практика проводится мастерами производственного обучения и (или) преподавателями общепрофессиональных дисциплин профессионального цикла, которые должны иметь высшее образование, соответствующее профилю преподаваемой дисциплины (модуля) и опыт деятельности в организациях соответствующей профессиональной сферы. Преподаватели должны проходить стажировку в профильных организациях не реже одного раза в три года.

Мастера производственного обучения: наличие 4-5 квалификационного разряда с обязательной стажировкой в профильных организациях не реже 1-го раза в 3 года. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным.

## 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Текущий контроль и оценка результатов освоения учебной практики осуществляется руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися учебно-производственных заданий, выполнения практических проверочных работ. В результате освоения учебной практики в рамках профессиональных модулей обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

| **Результаты (освоенные умения, первоначальный практический опыт в рамках ВПД)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| Эксплуатация автоматизированных (информационных) систем в защищенном исполнении | **Первоначальный практический опыт в:**<br><br>эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;<br><br>администрировании автоматизированных систем в защищенном исполнении;<br><br>установке компонентов систем защиты информации автоматизированных информационных систем.<br><br>**Умения:**<br><br>обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку | Текущий контроль в форме:<br>-устного опроса<br>- наблюдение за организацией рабочего места<br>- наблюдение и оценка практических работ<br>- экспертная оценка практических работ<br>-анализ результатов практических работ<br><br>Промежуточная аттестация (дифференцированный зачёт).<br><br>Текущий контроль в форме:<br>-устного опроса<br>- наблюдение за организацией рабочего места<br>- наблюдение и оценка |

| | | |
|---|---|---|
| | автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;<br><br>производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;<br><br>организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;<br><br>настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам. | практических работ<br>- экспертная оценка практических работ<br>-анализ результатов практических работ<br><br>Промежуточная аттестация (дифференцированный зачёт). |
| Защита информации в автоматизированных системах программными и программно-аппаратными средствами | **Первоначальный практический опыт в:**<br><br>установке и настройке программных средств защиты информации;<br><br>тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;<br><br>учете, обработке, хранении и передаче информации, для | Текущий контроль в форме:<br>-устного опроса<br>- наблюдение за организацией рабочего места<br>- наблюдение и оценка практических работ<br>- экспертная оценка практических работ<br>-анализ результатов практических работ<br><br>Промежуточная аттестация (дифференцированный |

| | | |
|---|---|---|
| | которой установлен режим конфиденциальности.<br><br>**Умения:**<br><br>устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;<br><br>диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;<br><br>проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;<br><br>использовать типовые программные криптографические средства, в том числе электронную подпись;<br><br>устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;<br><br>осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения | зачёт).<br><br>Текущий контроль в форме:<br>-устного опроса<br>- наблюдение за организацией рабочего места<br>- наблюдение и оценка практических работ<br>- экспертная оценка практических работ<br>-анализ результатов практических работ<br><br>Промежуточная аттестация (дифференцированный зачёт). |

| | | |
|---|---|---|
| | и ликвидации последствий компьютерных атак. | |
| Защита информации техническими средствами | **Первоначальный практический опыт в:**<br>выявлении технических каналов утечки информации;<br>применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;<br>проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;<br>проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.<br>**Умения:**<br>применять средства охранной сигнализации, охранного телевидения и | Текущий контроль в форме:<br>-устного опроса<br>- наблюдение за организацией рабочего места<br>- наблюдение и оценка практических работ<br>- экспертная оценка практических работ<br>-анализ результатов практических работ<br>Промежуточная аттестация (дифференцированный зачёт).<br>Текущий контроль в форме:<br>-устного опроса<br>- наблюдение за организацией рабочего |

| | | |
|---|---|---|
| | систем контроля и управления доступом;<br>применять технические средства для криптографической защиты информации конфиденциального характера;<br>применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;<br>применять инженерно-технические средства физической защиты объектов информатизации. | места<br>- наблюдение и оценка практических работ<br>- экспертная оценка практических работ<br>-анализ результатов практических работ<br><br>Промежуточная аттестация (дифференцированный зачёт). |
| Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин | **Первоначальный практический опыт:**<br>выполнения требований техники безопасности при работе с вычислительной техникой;<br>организации рабочего места оператора электронно-вычислительных и вычислительных машин;<br>подготовки оборудования компьютерной системы к работе;<br>инсталляции, настройки и обслуживания программного обеспечения компьютерной системы; | Текущий контроль в форме:<br>тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике<br><br>Промежуточная аттестация (дифференцированный зачёт). |

| | | |
|---|---|---|
| | управления файлами;<br>применения офисного программного обеспечения в соответствии с прикладной задачей;<br>использования ресурсов локальной вычислительной сети;<br>использования ресурсов, технологий и сервисов Интернет;<br>применения средств защиты информации в компьютерной системе.<br>**Умения:**<br>выполнять требования техники безопасности при работе с вычислительной техникой;<br>производить подключение блоков персонального компьютера и периферийных устройств;<br>производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники;<br>диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники;<br>выполнять инсталляцию системного и прикладного программного обеспечения;<br>создавать и управлять | Текущий контроль в форме:<br>тестирование,<br>экспертное наблюдение выполнения лабораторных работ,<br>экспертное наблюдение выполнения практических работ,<br>оценка решения ситуационных задач,<br>оценка процесса и результатов выполнения видов работ на практике<br>Промежуточная аттестация (дифференцированный зачёт). |

| | | |
|---|---|---|
| | содержимым документов с помощью текстовых процессоров;<br><br>создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц;<br><br>создавать и управлять содержимым презентаций с помощью редакторов презентаций;<br><br>использовать мультимедиа проектор для демонстрации презентаций;<br><br>вводить, редактировать и удалять записи в базе данных;<br><br>эффективно пользоваться запросами базы данных;<br><br>создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики;<br><br>производить сканирование документов и их распознавание;<br><br>производить распечатку, копирование и тиражирование документов на принтере и других устройствах;<br><br>управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете;<br><br>осуществлять навигацию по | |

| | | |
|---|---|---|
| | Веб-ресурсам Интернета с помощью браузера;<br><br>осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов;<br><br>осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ;<br><br>осуществлять резервное копирование и восстановление данных | |