

**ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ  
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ «КОЛЛЕДЖ СВЯЗИ № 54» ИМЕНИ П.М.ВОСТРУХИНА**

**РАБОЧАЯ ПРОГРАММА  
УЧЕБНОЙ ПРАКТИКИ**

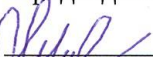
**ПМ 03. Применение инженерно-технических средств обеспечения  
информационной безопасности.**

По специальности **090305 «Информационная безопасность  
автоматизированных систем»**

Москва  
2016

РЕКОМЕНДОВАНА

Методической цикловой комиссией  
Протокол № 1 от «29» августа 2016 г.


Председатель ЦМК  
 М.Ф. Новикова

«29»августа 2016 г.

УТВЕРЖДАЮ

Зам. директора по УПР

ГБПОУ КС № 54 им. П.М.  
Вострухина

  
О.В. Корешков

«29»августа 2016 г.

Разработчики:

Сучков Д.А. мастер производственного обучения

Шпаков М.А. мастер производственного обучения

---

Ф.И.О., должность

Рецензенты:

---

Ф.И.О., должность

## СОДЕРЖАНИЕ

| СТР. |  |
|------|--|
|      | 1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ..... 4                   |
|      | 2. РЕЗУЛЬТАТЫ УЧЕБНОЙ ПРАКТИКИ..... 7                          |
|      | 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОЙ<br>ПРАКТИКИ..... 9 |
|      | 4 УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ПРАКТИКИ..... 23            |
|      | 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРАКТИКИ..... 26              |

# 1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

## 1.1. Место учебной практики в структуре основной профессиональной образовательной программы (далее - ОПОП).

Программа учебной практики является частью ОПОП и подразумевает готовность обучающегося к выполнению вида профессиональной деятельности **Применение инженерно-технических средств обеспечения информационной безопасности.**

- Применение инженерно-технических средств обеспечения информационной безопасности;
- Ремонт и техническое обеспечение сетевого оборудования;
- Организация и защита беспроводных систем передачи

## 1.2. Цели и задачи учебной практики

Учебная практика направлена на формирование у обучающихся первоначальных практических профессиональных умений, приобретение первоначального практического опыта. Реализуется в рамках модулей ОПОП СПО по основным видам профессиональной деятельности для освоения рабочей профессии, обучения трудовым приемам, операциям и способам выполнения трудовых процессов, характерных для соответствующей профессии и необходимых для последующего освоения ими общих и профессиональных компетенций по избранной профессии.

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

### **Вид профессиональной деятельности:**

**Выполнение работ по инженерно-техническим средствам обеспечивающих информационную безопасность**

**иметь практический опыт:**

**монтажа, эксплуатации и обслуживания локальных компьютерных сетей;**

**Уметь:**

- применять технические средства защиты информации;
- использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;
- использовать средства защиты информации от несанкционированного съёма и утечки по техническим каналам;
- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами.

**Знать:**

- физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации;
- основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам;
- номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

**Вид профессиональной деятельности:**

**Выполнение работ по ремонту и техническому обеспечению сетевого оборудования**

**иметь практический опыт:**

- установки и настройки сетевого и серверного оборудования для подключения к глобальным компьютерным сетям (Интернет);
- установки и настройки программного обеспечения для работы с ресурсами и сервисами;
- диагностики и мониторинга параметров сетевых подключений, устранения простейших неисправностей и сбоев в работе;
- Физический ремонт сетевого оборудования

**уметь:**

- устанавливать и настраивать подключения к Интернету с помощью различных технологий и специализированного оборудования;
- осуществлять ремонт оборудования;
- Диагностировать не исправности

**знать:**

- Элементарную базу радиодеталей
- Разновидность оборудования
- Типовые признаки не исправности и их устранения

**Вид профессиональной деятельности:**

## **Организация и защита беспроводных систем передачи**

### **иметь практический опыт:**

- обеспечения информационной безопасности беспроводных компьютерных сетей,
- установки, настройки и эксплуатации антивирусных программ;
- противодействия возможным угрозам информационной безопасности.

### **уметь:**

- осуществлять меры по защите компьютерных сетей от несанкционированного доступа;
- применять специализированные средства для борьбы с несанкционированным доступом к беспроводным сетям
- вести отчетную и техническую документацию.

### **знать:**

- виды угроз и методы защиты беспроводных сетей
- аппаратные и программные средства защиты беспроводных сетей;
- методы обеспечения защиты беспроводных сетей от несанкционированного доступа;
- состав мероприятий по защите персональных данных.

### **1.3. Количество недель (часов) на освоение программы учебной практики:**

В рамках освоения ПМ03. – 72 часа

## 2. РЕЗУЛЬТАТЫ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения рабочей программы учебной практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках модулей ОПОП СПО по основным видам профессиональной деятельности (ВПД)

1. Применение инженерно-технических средств обеспечения информационной безопасности;
2. Ремонт и техническое обеспечение сетевого оборудования;
3. Организация и защита беспроводных систем передаче необходимых для последующего освоения ими общих компетенций (ОК)

| Код    | Наименование результата практики  |
|--------|---|
| ОК 1.  | Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес   |
| ОК 2.  | Организовывать собственную деятельность, исходя из цели и способов ее достижения, определенных руководителем  |
| ОК 3.  | Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности. Нести ответственность за результаты своей работы   |
| ОК 4.  | Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.  |
| ОК 5.  | Использовать информационно-коммуникационные технологии в профессиональной деятельности  |
| ОК 6.  | Работать в команде, эффективно общаться с коллегами, руководством, клиентами.   |
| ОК 7.  | Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей)   |
| ОК 8.  | Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий   |
| ОК 9.  | Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации  |
| ОК 10. | Ориентироваться в условиях частой смены технологий в профессиональной деятельности  |
| ОК 11. | Формулировать задачи логического характера и применять средства математической логики для их решения  |
| ОК 12. | Владеть основными методами и средствами разработки программного обеспечения   |
| ОК 13. | Производить установку и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах |

и профессиональных компетенций (ПК)

| <b>Вид профессиональной деятельности</b>  | <b>Код</b> | <b>Наименование результатов практики</b>   |
|---|------------|--|
| <b>Применение инженерно-технических средств обеспечения информационной безопасности</b> | ПК3.1      | Применять инженерно-технические средства обеспечения информационной безопасности.  |
|   | ПК3.2      | Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности |
|   | ПК3.3      | Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности  |
|   | ПК3.4      | Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.   |
|   | ПК3.5      | Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами  |



### 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

#### 3.1. Тематический план

| Код ПК                  | Код и наименование профессионального модуля   | Количество часов практики по ПМ | Наименование разделов учебной практики   | Количество часов по темам |
|-------------------------|---|---------------------------------|--|---------------------------|
| 1                       | 2   | 3                               | 4  | 5                         |
| ПК<br>3.1-<br>ПК<br>3.5 | ПМ03 Применение инженерно-технических средств обеспечения информационной безопасности | 30                              | Раздел 1. Применение инженерно-технических средств обеспечения информационной безопасности | 18                        |
|                         |   | 18                              | Раздел 2. Ремонт и техническое обеспечение сетевого оборудования                           | 36                        |
|                         |   | 24                              | Раздел 3. Организация и защита беспроводных систем передачи информации                     | 18                        |
| <b>ВСЕГО</b>            |   |                                 |  | <b>72</b>                 |

### 3.2. Содержание учебной практики

| Код и наименование профессиональных модулей, разделов и тем учебной практики                      | Содержание учебных занятий  | Объем часов | Уровень освоения |
|---|---|-------------|------------------|
| 1   | 2   | 3           | 4                |
| <b>ПМ03 Применение инженерно-технических средств обеспечения информационной безопасности</b>      |   | <b>72</b>   |                  |
| <b>Раздел 1. Применение инженерно-технических средств обеспечения информационной безопасности</b> |   | 30          |                  |
| <b>УП 03. Тема 1.1. Техника безопасности и охрана труда</b>                                       | Электра безопасность. Пожара безопасность. Охрана труда на рабочем месте. Первая медицинская помощь.  | 6           | 2                |
| <b>УП 03. Тема 1.2. Информация и каналы утечки информации</b>                                     | <p>Понятие информации, защиты информации, информационной системы, безопасности автоматизированных систем обработки информации. Цель защиты информации.</p> <p>Базовые свойства информации: конфиденциальность, целостность, доступность.</p> <p>Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя.</p> <p>Причины несанкционированного доступа к информации.</p> <p>Последствия несанкционированного доступа к информации.</p> <p>Понятие угрозы, классификация угроз.</p> <p>Понятие уязвимости, атаки на компьютерную систему.</p> <p>Понятие риска. Задача специалиста по информационной безопасности.</p> <p>Виды утечки информации. Понятие канала утечки информации, основные каналы утечки информации и пути их возникновения.</p> <p>Классификация злоумышленников;</p> <p>Акустические каналы утечки информации;</p> | 6           | 2                |
| <b>УП 03. Тема 1.3.</b>   | <p>Подсистемы разграничения доступа к ресурсам.</p> <p>Цели применения криптографических преобразований, электронно-цифровой подписи.</p> <p>Аудит безопасности, резервирование ресурсов и компонентов автоматизированной системы.</p>  | 6           | 2                |

|  |  |   |   |
|--|--|---|---|
|  | <p>Типы аппаратуры в технических каналах утечки информации</p> <p>Классификация инженерно-технических средств</p> <p>Устройства идентификации iButton. История развития, внешний вид и структура электронного ключа iButton. Области применения, принципы конструкции iButton.</p> <p>Бесконтактные радиочастотные карты proximity. Внешний вид и принцип работы карт, пассивные и активные карты.</p> <p>Пластиковые карты. Внешний вид и классификация пластиковых карт: карты со штрих кодом, карты с магнитной полосой, карты-счетчики, карты с памятью, карты с микропроцессором.</p> <p>Понятие и примеры биометрических характеристик человека, особенность применения биометрических систем идентификации и аутентификации личности по сравнению с другими классами систем идентификации и аутентификации, коэффициент ошибочных отказов и ошибочных подтверждений, архитектура биометрических систем аутентификации, обучение биометрических систем.</p> <p>Системы перехвата и анализа сигналов</p> <p>Характеристики аппаратуры в технических каналах утечки информации</p> <p>Работоспособность инженерно-технических средств обеспечения информационной безопасности</p> <p>Причины отказов работоспособности</p> <p>Классификация проблем инженерно-технических средств обеспечения информационной безопасности</p> <p>Устранения отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности</p> |   |   |
| <p><b>УП 03. Тема 1.4</b><br/><b>Методы и средства технической защиты информации</b></p> | <p>Концепция и методы инженерно-технической защиты информации;</p> <p>Экранирование электромагнитных волн ;Экранированные помещения;</p> <p>Безопасность оптоволоконных кабельных систем. Заземление технических средств и подавление информационных сигналов в цепях заземления ;Фильтрация информационных сигналов; Основные сведения о помехоподавляющих фильтрах; Выбор типа фильтра; Пространственное и линейное зашумление.; Устройства контроля и защиты слаботоочных линии и сети; Особенности слаботоочных линии и сетей как каналов утечки информации ;Рекомендуемые схемы подключения анализаторов к электросиловым и телефонным линиям в здании Устройства контроля и защиты проводных линии от утечки информации ;Скрытие речевои информации в телефонных системах с использованием криптографических методов</p> <p>Системы шифрования информации; Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма. Принципы функционирования криптографической системы. Классификация криптосистем.Понятиекриптоанализа, криптоаналитической атаки. Основные типы криптоаналитических атак, криптостойкость шифра. Требования к шифрам, используемым для</p>  | 6 | 2 |

|   |  |           |   |
|---|--|-----------|---|
|   | криптографической защиты информации. Принцип функционирования асимметричных криптосистем, Функциональная схема взаимодействия участников асимметричного криптографического обмена. Достоинства и недостатки асимметричных криптосистем. Реализация двустороннего обмена ключевой информацией. Понятие и назначение центра распределения ключей   |           |   |
| <b>УП 03. Тема 1.5.<br/>Инженерная и техническая защита<br/>охраны объектов</b> | Категории объектов защиты; Особенности задач охраны различных типов объектов; Общие принципы обеспечения безопасности объектов; Система охранно-тревожной □ сигнализации; Система контроля и управления доступом; Телевизионные системы; Система пожарной □ сигнализации; Периметровая охрана. Номенклатуру применяемых средств охраны и безопасности; Системы видеонаблюдения Технические каналы утечки видовой □ информации; Способы скрытого видеонаблюдения и съемки; Общие сведения. Мероприятия по выявлению и оценке свойств каналов утечки информации; ; Специальные проверки; Специальные обследования; Специальные исследования; Специальные исследования акустических и виброакустических каналов ; Специальные исследования акустоэлектрических преобразовании □; Специальные исследования технических средств и систем на возможность утечки информации за счет побочных □ электромагнитных излучений □ и наводок | 6         | 2 |
| <b>Раздел 2. Ремонт и техническое обслуживание сетевого оборудования</b>        |  | <b>18</b> |   |
| <b>УП 03. Тема 2.1.<br/>Сетевые технологии</b>                                  | Локальные вычислительные сети. Сравнение узкополосных и широкополосных сетей. Сравнение коммутации пакетов и коммутации каналов. Сети и сетевые комплексы<br>Кабели и топологии. Управление доступом к среде передачи данных. Повторители и мосты. Коммутаторы и маршрутизаторы. Глобальные сети. Протоколы и стандарты.<br>Клиенты и серверы. Операционные системы и приложения   | 6         | 2 |
| <b>УП 03. Тема 2.2. Сетевое аппаратное обеспечение</b>                          | Платы сетевых адаптеров. Дополнительные возможности сетевых адаптеров. Полный дуплекс. Управление шиной.<br>Параллельное выполнение задач. Дистанционное включение.<br>Протокол. Скорость передачи. Сетевой интерфейс. Интерфейс шины. Требования к аппаратным ресурсам. Требования к электропитанию. Сетевые адаптеры для серверов. Сетевые адаптеры для рабочих станций.   | 6         | 2 |
| <b>УП 03. Тема 2.3.<br/>Прокладка сетевого кабеля</b>                           | Свойства кабеля. Стандарты кабельных систем. Стандарты протоколов канального уровня. Толстый кабель Ethernet. Тонкий кабель Ethernet. Технология ARCNET. Кабельное телевидение. Кабели на основе витой пары. Незэкранированная витая пара. Схема расположения контактов коннекторов. Оптоволоконный кабель. Строение оптоволоконного кабеля. Коннекторы для оптоволоконного кабеля. Прокладка кабеля<br>Монтаж оборудования. Тестирование соединений   | 6         | 2 |

|  |   |           |   |
|--|---|-----------|---|
| <b>Раздел 3. Организация и защита беспроводных систем передачи информации.</b>                             |   | <b>24</b> |   |
| <b>УП 03. Тема 3.1.<br/>Организационная структура системы обеспечения безопасности передачи информации</b> | Основы беспроводных сетей<br>Понятие технологии обеспечения безопасности передачи информации.<br>Институт ответственных за обеспечение безопасности передачи информации.  | 6         | 2 |
| <b>УП 03. Тема 3.2.<br/>Требования к защите передачи информации</b>  | Общие правила обеспечения безопасности передачи информации при работе сотрудников. Ответственность за нарушения.<br>Порядок работы с носителями ключевой информации.<br>Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов.<br>Категорирование защищаемых ресурсов.<br>Взаимодействие подразделений на всех этапах передачи информации | 6         | 2 |
| <b>УП 03. Тема 3.3.<br/>Обнаружение и устранение уязвимостей передачи информации.</b>                      | Архитектура систем управления уязвимостями<br>Особенности сетевых агентов сканирования<br>Специализированный анализ защищенности<br>Обзор средств анализа защищенности  | 6         | 2 |
| <b>УП 03. Тема 3.4.<br/>Средства защиты беспроводных сетей<br/>Дифференцированный зачет</b>                | Алгоритм привязки RADIUS-сервера к беспроводной сети<br>Лабораторная работа 18. Разработка комплекса защиты беспроводной сети:<br>MAC-аутентификация<br>Широковещательная передача SSID   | 6         | 2 |
| <b>ВСЕГО</b>   |   | <b>72</b> |   |

## 4. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ УЧЕБНОЙ ПРАКТИКИ

### 4.1 Требования к материально-техническому обеспечению

Реализация рабочей программы учебной практики предполагает наличие кабинета **информационных технологий**; лабораторий по профилю профессиональных модулей.

#### **Кабинет информационных технологий:**

Оборудование учебного кабинета и рабочих мест кабинета

- посадочных мест по количеству обучающихся в подгруппе 15;
- рабочее место преподавателя 1;
- образцы приборов, сетевого оборудования и примерная проектная документация;

Оборудование и технологическое оснащение рабочих мест:

- Компьютер обучающегося (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО, операционные системы Windows, UNIX, MSOffice, пакет САПР)
- Компьютер преподавателя (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное, операционные системы Windows, UNIX, MSOffice, пакет САПР)

Технические средства обучения:

- компьютеры с лицензионным программным обеспечением
- интерактивная доска
- проектор

#### **Лаборатория (по профилю практики):**

Оборудование лаборатории и рабочих мест лаборатории:

- Оборудование лаборатории и рабочих мест лаборатории: 15 компьютеров обучающихся и 1 компьютер преподавателя;
- Типовой состав для ремонта сетевого оборудования
- Пример проектной документации;
- Набор оборудования и средств для обеспечения информационной безопасности;
- Проектор

- Типовое активное и пассивное сетевое оборудование: сетевые маршрутизаторы, сетевые коммутаторы, сетевые хранилища, сетевые модули и трансиверы, шасси и блоки питания, шлюзы VPN, принт-серверы, сетевые адаптеры и карты, сетевые контроллеры, оборудование xDSL, аналоговые модемы, коммутационные панели, беспроводные маршрутизаторы, беспроводные принт-серверы, точки доступа WiFi;
- Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности.

#### **4.2 Перечень учебных изданий, Интернет ресурсов, дополнительной литературы**

Основные источники:

1. Виснадул П.Д., Лупин С. А., Сидоров С. В., Чумагина П. Ю. Основы компьютерных сетей. М.: Форум, ИНФРА – М, 2007.
2. Максимов Н.В., Попов И.И. Компьютерные сети. М.: Форум, 2008.
3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2010.
4. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. М.: Академия, 2007.
5. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность. М.: Академия, 2010.

Дополнительные источники:

1. Анкудинов Г.И., Анкудинов И.Г., Стрижаченко А.И. Сети ЭВМ и телекоммуникации. Архитектура и сетевые технологии. СПб.: СЗТУ, 2006.
2. Ватаманюк А. Создание, обслуживание и администрирование сетей. СПб.: Питер, 2008.
3. Глушаков С. В. Хачиров Т. С. Настраиваем сеть своими руками-М: ФОЛИР, 2008.
4. Поляк-Брагинский А.В. Локальные сети. Модернизация и поиск неисправностей. СПб.: БХВ-Петербург, 2006.
5. Попов В.Б. Основы информационных и телекоммуникационных технологий. Сетевые информационные технологии. М.: Финансы и статистика, 2005.

#### **4.3. Требования к руководителям практики от образовательного учреждения.**

Учебная практика проводится мастерами производственного обучения, зав. лабораторией или преподавателями профессионального цикла.

#### **4.4. Кадровое обеспечение образовательного процесса**

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



## 5. Контроль и оценка результатов освоения программы учебной практики

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

| Результаты обучения<br>(освоенные умения в рамках ВПД)   | Формы и методы контроля и оценки<br>результатов обучения  |
|--|---|
| <b>Выполнение работ по монтажу, наладке, эксплуатации обслуживанию локальных компьютерных сетей:</b><br><b>уметь:</b> <ul style="list-style-type: none"><li>- осуществлять монтаж кабельной сети и оборудования локальных сетей различной топологии;</li><li>- осуществлять монтаж беспроводной сети и оборудования локальных сетей различной топологии;</li><li>- осуществлять диагностику работы локальной сети;</li><li>- подключать сервера, рабочие станции, принтеры и другое сетевое оборудование к локальной сети;</li><li>- выполнять работы по эксплуатации и обслуживанию сетевого оборудования;</li><li>- обеспечивать работу системы регистрации и авторизации пользователей сети;</li><li>- осуществлять системное администрирование локальных сетей;</li><li>- вести отчетную и техническую документацию;</li></ul> | Экспертная оценка деятельности обучающихся во время проведения этапов учебной практики, выполнения ими самостоятельных заданий.<br>Зачет. |