Министерство образования и молодежной политики Свердловской области

государственное автономное профессиональное образовательное учреждение Свердловской области «Уральский радиотехнический колледж им. А.С. Попова»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

# ПМ.01 Эксплуатация подсистем безопасности автоматизированных систем

для специальности среднего профессионального образования

10.02.03 Информационная безопасность автоматизированных систем

базового уровня подготовки

2020 г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования

10.02.03 Информационная безопасность автоматизированных систем

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Д.В. Колесников

«30» июня 2020 г.

Рекомендована цикловой методической комиссией
«Электронных вычислительных машин»
Протокол от «29 » июня 202019 г. № 6

Председатель ЦМК _____ Ю.Г. Котова

Разработчики:

Уймин А.Г., преподаватель УРТК им. А. С. Попова

СОДЕРЖАНИЕ

# 1 ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## ПМ. 01 Эксплуатация подсистем безопасности автоматизированных систем

### 1.1 Область применения программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.03 «Информационная безопасность автоматизированных систем» в части освоения основного вида профессиональной деятельности (ВПД) «Эксплуатация подсистем безопасности автоматизированных систем» и соответствующих профессиональных компетенций (ПК):

–ПК 1.1. участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности;

–ПК 1.2. выполнять работы по администрированию подсистем безопасности автоматизированных систем;

–ПК 1.3. производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем;

–ПК 1.4. организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них;

–ПК 1.5. вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах.

### 1.2 Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

**иметь практический опыт:**

–эксплуатации компонентов подсистем безопасности автоматизированных систем, их диагностики, устранения отказов и восстановления работоспособности;

–администрирования подсистем безопасности автоматизированных информационных систем;

–установки компонентов подсистем безопасности автоматизированных информационных систем;

**уметь:**

–эксплуатировать компоненты подсистем безопасности автоматизированных систем;

–обеспечивать работоспособность, обнаруживать и устранять неисправности подсистем безопасности автоматизированных систем согласно технической документации;

–осуществлять комплектование, конфигурирование, настройку подсистем безопасности автоматизированных систем;

–производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав подсистемы безопасности автоматизированной системы;

–использовать и оформлять техническую документацию в соответствии с действующими нормативными документами;

–выполнять регламенты техники безопасности;

–организовывать и конфигурировать компьютерные сети;

–работать с протоколами разных уровней;

–устанавливать и настраивать параметры современных сетевых протоколов;

–производить монтаж компьютерных сетей;

–осуществлять диагностику компьютерных сетей;

–устранять неисправности компьютерных сетей;

**знать:**

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

–принципы разработки алгоритмов программ;

–основные приемы программирования;

–модели баз данных;

–классификацию, принципы построения, физические основы работы периферийных устройств;

–основные методы организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;

–правила и нормы охраны труда, техники безопасности, промышленной санитарии и противопожарной защиты;

–основные понятия компьютерных сетей и их аппаратные компоненты;

–сетевые модели, протоколы и их установку в операционных системах;

–адресацию в сетях, организацию межсетевого воздействия.

**1.3 Количество часов на освоение программы профессионального модуля:**

всего – 616 курс проект часов, в том числе:

- максимальной учебной нагрузки обучающегося 436 часов, включая:
- обязательной аудиторной учебной нагрузки обучающегося – 290 часов;
- самостоятельной работы обучающегося – 146 часов;

-учебной практики – 180 часов

## 2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения рабочей программы профессионального модуля является овладение обучающимися видом профессиональной деятельности «Эксплуатация подсистем безопасности автоматизированных систем», в том числе профессиональными (ПК) и общими (ОК) компетенциями:

| Код | Наименование результата обучения |
|---|---|
| ПК 1.1 | Участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности. |
| ПК 1.2 | Выполнять работы по администрированию подсистем безопасности автоматизированных систем. |
| ПК 1.3 | Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем. |
| ПК 1.4 | Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них. |
| ПК 1.5 | Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах. |
| ОК 1 | Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности. |
| ОК 2 | Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. |
| ОК 3 | Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. |
| ОК 4 | Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. |
| ОК 5 | Использовать информационно-коммуникационные технологии в профессиональной деятельности. |
| ОК 6 | Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. |
| ОК 7 | Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. |
| ОК 8 | Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| ОК 9 | Ориентироваться в условиях частой смены технологий в профессиональной деятельности. |
| ОК 10 | Формулировать задачи логического характера и применять средства математической логики для их решения. |

| Код | Наименование результата обучения |
|---|---|
| ОК 11 | Владеть основными методами и средствами разработки программного обеспечения. |
| ОК 12 | Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах. |

## 3 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
## ПМ. 01 Эксплуатация подсистем безопасности автоматизированных систем

### 3.1 Тематический план профессионального модуля

| Коды профессиональных компетенций | Наименования разделов профессионального модуля* | Всего часов | Объем времени, отведенный на освоение междисциплинарного курса (курсов) | | | | | Практика | |
|---|---|---|---|---|---|---|---|---|---|
| | | | Обязательная аудиторная учебная нагрузка обучающегося | | | Самостоятельная работа обучающегося | | Учебная, часов | Производственная (по профилю специальности), часов |
| | | | Всего, часов | в т.ч. лабораторные работы и практические занятия, часов | в т.ч., курсовая работа (проект), часов | Всего, часов | в т.ч., курсовая работа (проект), часов | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| ПК1.1, ПК1.2, ПК1.3, ПК1.4 | **Раздел 1 Эксплуатация подсистем безопасности автоматизированных систем** | **254** | **96** | 24 | - | **50** | - | **108** | - |
| ПК1.1, ПК1.2, ПК1.3, ПК1.5 | **Раздел 2 Эксплуатация компьютерных сетей** | **362** | **194** | 40 | 30 | **96** | 28 | **72** | |
| | **Производственная практика (по профилю специальности)**, часов | - | | | | | | | - |
| | **Всего:** | **616** | **290** | 64 | 30 | **146** | 28 | **180** | - |

## 3.2Содержание обучения по профессиональному модулю (ПМ)

| Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем | Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) | Объем часов | Уровень освоения |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **Раздел 1 Эксплуатация подсистем безопасности автоматизированных систем** | | **254** | |
| **МДК.01.01 Эксплуатация подсистем безопасности автоматизированных систем** | | **146** | |
| **Тема 1.1 Обзор технологий и развертывание системы защиты** | **Содержание** | 14 | |
| | 1. Назначение комплекса. | | 2 |
| | 2. Защитные механизмы. | | 2 |
| | 3. Аппаратные модули, архитектура системы, производительность для типовых платформ. | | 2 |
| | 4. Программные модули. | | 2 |
| | 5. ПАК "Соболь" | | 2 |
| | 6. Политика лицензирования. | | 2 |
| | **Лабораторные работы** | 8 | |
| | 1. Установка и инициализация ЦУС | | |
| | 2. Установка подсистемы управления комплексом | | |
| | 3. Конфигурирование базы данных журналов, настройка агента ЦУС и СД | | |
| | 4. Установка и инициализация КШ | | |
| **Тема 1. 2 Управление компонентами комплекса.** | **Содержание** | 6 | |
| | 1. Управление криптографическими ключами комплекса | | 2 |
| | 2. Локальное управление сетевыми устройствами | | 2 |
| | **Лабораторные работы** | 4 | |
| | 1. Создание учетной записи администратора | | |
| | 2. Смена главного ключа КШ и ключа связи с ЦУС | | |
| **Тема 1.3 Управление политиками безопасности** | **Содержание** | 10 | |
| | 1. Межсетевой экран. Принцип действия | | 2 |
| | 2. Формирование правил фильтрации трафика. | | 2 |
| | 3. Трансляция сетевых адресов (правила NAT). | | 2 |
| | 4. Пользовательские и автоматические правила. | | 2 |
| | **Лабораторные работы** | 8 | |
| | 1. Настройка правил фильтрации, разрешающих прохождение трафика между компьютерами из защищаемой сети и сети общего доступа | | |

| 1 | 2 | | 3 | 4 |
|---|---|---|---|---|
| | 2. | Настройка правила фильтрации, разрешающего прохождение трафика между компьютерами из внутренних сетей, защищаемых разными криптошлюзами | | |
| | 3. | Настройка исходящего правила трансляции | | |
| **Тема 1.4 Организация и управление VPN-соединениями.** | **Содержание** | | 8 | |
| | 1. | Организация VPN -шлюза. | | 2 |
| | 2. | VPN удаленного доступа. | | 2 |
| | **Лабораторные работы** | | 4 | |
| | 1. | Организация L3VPN | | |
| | 2. | Организация L2VPN | | |
| **Тема 1. 5 Обеспечение отказоустойчивости комплекса.** | **Содержание** | | 4 | |
| | 1. | Резервное копирование и восстановление конфигурации ЦУС. | | 2 |
| | 2. | Аппаратное резервирование и восстановление КШ. | | 2 |
| **Тема 1.6 Мониторинг и диагностика системы защиты.** | **Содержание** | | 4 | |
| | 1. | Мониторинг состояния комплекса. | | 2 |
| **Тема 1.7 Обновление версии ПО** | **Содержание** | | 4 | |
| | 1. | Обновление текущей версии ПО. | | 2 |
| | 2. | Требования к эксплуатации комплекса. | | 2 |
| **Тема 1. 8 Описание vGate** | **Содержание** | | 6 | |
| | 1. | Принципы и средства защиты | | 2 |
| | 2. | Функциональные возможности | | 2 |
| | 3. | Правила использования лицензий | | 2 |
| **Тема 1.9 Архитектура и компоненты vGate** | **Содержание** | | 6 | |
| | 1. | Компоненты и модули vGate | | 2 |
| | 2. | Варианты размещения | | 2 |
| | 3. | Совместимость с другими продуктами | | 2 |
| **Тема 1. 10 Развертывание отказоустойчивого кластера серверов vCenter** | **Содержание** | | 4 | |
| | 1. | Устройство кластера | | 2 |
| | 2. | Создание отказоустойчивого кластера | | 2 |
| **Тема 11 Защита кластера серверов с помощью vGate** | **Содержание** | | 4 | |
| | 1. | Добавление узлов кластера в список защищаемых объектов | | 2 |
| | 2. | Установка компонента защиты vCenter на узлы кластера. Удаление компонента защиты | | 2 |
| **Дифференцированный зачет** | | | **2** | |
| **Самостоятельная работа при изучении раздела 1 ПМ 01**<br>Систематическая проработка конспектов занятий, учебной литературы по главам и параграфам, указанным преподавателем.<br>Подготовка к лабораторным работам и практическим занятиям с использованием методических указаний преподавателя, оформление отчетов и подготовка к защите.<br>Оформление технической документации с использованием нормативных документов и государственных стандартов. | | | 50 | |

| 1 | 2 | | 3 | 4 |
|---|---|---|---|---|
| **Примерная тематика домашних заданий**<br>1 Изучение литературы<br>2. Подготовка к тестированию.<br>3.Офомление отчета по лабораторной работе.<br>4 Подготовка к защите лабораторной работы. | | | | |
| **УП.01.01 Учебная практика по работе с сетевыми операционными системами**<br>**Виды работ**<br>1.Разграничение прав доступа<br>2.Работа с центром безопасности сетевых ОС<br>3.DHCP-сервер: установка и управление<br>4.DNS-сервер: установка и управление<br>5.Создание основного и резервного контроллера домена Windows<br>6.Создание основного и резервного контроллера домена Windows Server<br>7.Создание и администрирование учетных записей пользователей и групп в домене Windows<br>8.Групповые политики<br>9.Администрирование файлового сервера<br>10.Автономные файлы. Службы DFS<br>11.Технология теневого копирования данных<br>12.Архивация данных<br>13.Службы IIS 8.0 установка и основы администрирования FTP-сервера<br>14.Удаленное управление Windows Server<br>15.Автоматическое обновление ОС с использованием службы WSUS<br>16.Шифрование файлов EFS<br>17.Локальные политики безопасности<br>18.Шифрование диска<br>19.Создание центра сертификации (Удостоверяющего центра)<br>20.Шифрование экспертной системы MSAT<br>21.Реестр Windows<br>22.Дифференцированный зачет | | | **108** | |
| **Раздел 2 Эксплуатация компьютерных сетей** | | | **362** | |
| **МДК.01.02Эксплуатация компьютерных сетей** | | | **290** | |
| **Тема 2. 1 Угрозы сетевой безопасности** | **Содержание** | | 24 | |
| | 1. | Современные угрозы сетевой безопасности | | 2 |
| | 2. | Вирусы, черви и троянские кони | | 2 |
| | 3. | Методы проведения сетевых атак | | 2 |
| | 4. | Безопасный доступ к устройствам | | 2 |
| | 5. | Назначение административных ролей | | 2 |
| | 6. | Мониторинг и управление устройствами | | 2 |
| **Тема 2.2 Базовые настройки безопасности активного сетевого оборудования** | **Содержание** | | **60** | |
| | 1. | Использование функции автоматизированной настройки безопасности | | 2 |

| 1 | 2 | | 3 | 4 |
|---|---|---|---|---|
| | 2. | Свойства AAA | | 2 |
| | 3. | Схема аутентификации без aaa new-model. Локальная AAA аутентификация | | 2 |
| | 4. | Server-based AAA | | 2 |
| | 5. | Настройка аутентификации для метода group | | 2 |
| | 6. | Технология брандмауэра, ACL | | 2 |
| | 7. | Dynamic ACL, Reflexive ACL, Time-based ACL | | 2 |
| | 8. | Контекстный контроль доступа (CBAC), Политики брандмауэра основанные на зонах | | 2 |
| | 9. | IPS технологии. Классификация, порядок настройки. IPS сигнатуры. | | 2 |
| | 10. | Реализация IPS. Проверка и мониторинг вторжений средствами IPS | | 2 |
| | 11. | Для чего не предназначены МЭ | | 2 |
| | 12. | Начальная настройка: маршрутизация, удаленное управление, списки контроля доступа, трансляция сетевых адресов. | | 2 |
| | 13. | Обеспечение безопасности рабочих мест пользователей | | 2 |
| | 14. | Безопасность на канальном уровне (Layer-2) Rogue DHCP Server, DHCP starvation, CAM-table overflow, VLAN hopping, MAC-spoofing | | 2 |
| | 15. | Настройка защиты от типовых атак канального уровня | | 2 |
| | **Лабораторные работы** | | 16 | |
| | 1. | Настройка безопасного доступа до маршрутизатора | | |
| | 2. | Безопасный административный доступ с использованием модели AAA и сервера RADIUS | | |
| | 3. | Настройка Zone-Based Policy Firewalls | | |
| | 4. | Безопасность беспроводных сетей, VoIP и SAN | | |
| **Тема 2. 3 Инструменты организации виртуальных частных сетей** | **Содержание** | | 40 | |
| | 1. | Технология VPN. Типы VPN соединений: Site-to-site VPN. | | 2 |
| | 2. | Технология VPN. Типы VPN соединений: Remote-access VPN | | 2 |
| | 3. | Стек протоколов IPSec | | 2 |
| | 4. | Принципы безопасности сетевого дизайна. Безопасная архитектура сетевой инфраструктуры. | | 2 |
| | 5. | Управление информационными процессами и безопасность. Тестирование сети на уязвимости | | 2 |
| | 6. | Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование. | | 2 |
| | **Лабораторные работы** | | 24 | |
| | 1. | Настройка Site-to-Site VPN | | |
| | 2. | Настройка Remote Access VPN клиентской и серверной части | | |
| | 3. | Настройка Remote Access VPN клиентской и серверной частей. Динамическая маршрутизация | | |
| | 4. | Базовая настройка МЭ | | |

| 1 | 2 | | 3 | 4 |
|---|---|---|---|---|
| | 5. | Настройка Clientless and AnyConnect Remote Access SSL VPNs | | |
| | 6. | Настройка Site-to-Site IPsec VPN | | |
| **Курсовое проектирование** | 1. | КП1. Оформление задания. Состав пояснительной записки. | 30 | 3 |
| | 2. | КП2. Разработка введения. Требования к разделу. | | |
| | 3. | КП3. Описание протоколов файлового доступа и защищенного удаленного доступа | | |
| | 4. | КП4. Описание протоколов динамической маршрутизации и доменных имен. | | |
| | 5. | КП5. Описание протокола сетевого времени и WEB-сервера | | |
| | 6. | КП6. Описание протокола LDAP и почтового сервера. | | |
| | 7. | КП7. Выбор и обоснование системного программного обеспечения | | |
| | 8. | КП8. Развертывание системы виртуализации. Установка и начальная настройка ОС. | | |
| | 9. | КП9. Подготовка шаблона ОС. Настройка протоколов файлового доступа | | |
| | 10. | КП10. Настройка протокола защищенного удаленного доступа и сервера динамической маршрутизации | | |
| | 11. | КП11. Настройка сервера доменных имен и протокола сетевого времени. | | |
| | 12. | КП12. Настройка WEB-сервера и Free IPA | | |
| | 13. | КП13. Настройка почтового сервера | | |
| | 14. | КП14. Расчёт стоимости работ по настройке системы | | |
| | 15. | КП15. Расчёт стоимости работ по настройке системы | | |
| **Самостоятельная работа при изучении раздела 2 ПМ 01**<br>Систематическая проработка конспектов занятий, учебной литературы по главам и параграфам, указанным преподавателем.<br>Подготовка к лабораторным работам занятиям с использованием методических указаний преподавателя, оформление отчетов и подготовка к защите.<br>Оформление технической документации с использованием нормативных документов и государственных стандартов. | | | 96 | |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| **Примерная тематика домашних заданий**<br>1. Изучение литературы<br>2. Подготовка к тестированию.<br>3.Оформление отчета по лабораторной работе.<br>4.Подготовка к защите лабораторной работы.<br>5 Разработка и письменное оформление раздела «Введение»<br>6 Описать протоколы файлового доступа и защищенного удаленного доступа<br>7 Описать протоколы динамической маршрутизации и доменных имен.<br>8 Описать протокол сетевого времени и WEB-сервер<br>9 Описать протокол LDAP и почтовый сервер<br>10 Выбрать системное программное обеспечение<br>11 Развернуть систему виртуализации. Установить и настроить ОС.<br>12 Подготовить шаблон ОС и настроить протоколы файлового доступа.<br>13 Настроить протокол защищенного удаленного доступа и сервера динамической маршрутизации<br>14 Настроить сервер доменных имен и протокол сетевого времени<br>15 Настроить WEB-сервер и Free IPA<br>16 Настроить почтовый сервер<br>17 Рассчитать стоимость работ по настройке системы | | | |
| **Примерная тематика курсовых проектов**<br>1.Обеспечение безопасности работы сети на канальном уровне средствами управляемых коммутаторов<br>2.Обеспечение безопасности работы сети на канальном уровне средствами ASA 5505<br>3.Развертывание IP телефонии на базе оборудования Cisco<br>4.Развертывание беспроводной сети на базе оборудования Cisco | | | |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | | **72** | |
| **УП.01.02 Учебная практика по администрированию операционных систем**<br>**Виды работ**<br>1.Доступ к командной строке<br>2.Управление файлами при помощи командной строки<br>3.Получение помощи в Linux<br>4.Создание, просмотр и редактирование текстовых файлов<br>5.Управление локальными пользователями и группами Linux<br>6.Управление доступом к файлам при помощи разрешений файловой системы Linux<br>7.Мониторинг и управление процессами в Linux<br>8.Управление сервисами и демонами<br>9.Настройка и обеспечить безопасности OpenSSH<br>10.Анализ и хранение лог-файлов<br>11.Настройка сети в Linux<br>12.Архивирование и копирование файлов между системами<br>13.Установка и обновление программных пакетов<br>14.Доступ к файловым системам Linux<br>15.Использование виртуальных систем<br>16.Автоматизация установки<br>17.Использование регулярных выражение в grep<br>18.Создание и редактирование текстовых файлов в vim<br>19.Выполнение задач по расписанию<br>20.Управление приоритетами процессов Linux<br>21.Контроль доступа к файлам с использованием списков контроля доступа<br>22.Управление безопасностью Linux<br>23.Подключение с использованием сетевых пользователей и групп<br>24.Добавление дисков, разделов и файловых систем<br>25.Получение доступа к сетевым хранилищам с использованием Network File System<br>26.Получение доступа к сетевым хранилищам с использованием SMB<br>27.Ограничение сетевых коммуникаций с использованием брандмауэра<br>28.Управление сетями на базе IPv6<br>29.Управление DNS<br>30.Настройка веб-службы Apache HTTPD<br>31.Настройка доставки электронной почты<br>32.Настройка среды<br>33.Дифференцированный зачет | | | |
| | **Всего:** | **656** | |

1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

# 4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## 4.1 Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы модуля предполагает наличие лаборатории «Программно-аппаратных средств обеспечения информационной безопасности» и мастерской «Корпоративная защита от внутренних угроз информационной безопасности».

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

– Персональный компьютер с аппаратной поддержкой виртуализации и техническими характеристиками не ниже i7\16 Gb \SSD 128\HDD 1 Tb\VGA integrate\ Monitor 23”;

– программное обеспечение VirtualBox, KVM ;

– программное обеспечение OpenOffice;

– АПКШ «Континент»;

– комплекс vGate;

– Аппаратное обеспечение ISR G2 (Cisco 2901);

– Аппаратное обеспечение Cisco Catalyst WS-2960+24TC-L;

– Аппаратное обеспечение Cisco ASA 5505;

– проектор;

– столы и стулья.

Оборудование лаборатории и рабочих мест мастерской «Корпоративная защита от внутренних угроз информационной безопасности»:

– ПЭВМ в сборе (i7/32Gb MEM/ 256Gb + 1Tb nvme SSD/ Nvidia Qadro 1000 / Intel 4x1Gb/s Lan Card/ 27” Monitor)

– ViPNet Software (Coordinator for Windows 4.x + Client for Windows 4.x + Policy Manager 4.x + VPN HW Router )

– Видео проектор Epson EB-2247U

– Экран для проектора Lumien Master Picture 191x300 Matte White FiberGlass

– Рабочее место в сборе:

- стол (ШхД) 1800x750;

- рама задняя короткая;

- перфопанель – 2;

- набор держателей;

- электроблок на 8 розеток;1

- полка приборная длинная;

- светильник светодиодный – 2 шт;

- кронштейн для монитора – 2 шт;

- полка для системного блока – 2 шт;

- стул тканевый с металлической крестовиной – 2 шт;

- металлические колеса для стула – 2 шт;

- набор подлокотников – 2 шт.

### 4.2 Информационное обеспечение обучения

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы**

Основные источники:

1.Староверова, Н.А. Операционные системы [Электронный ресурс] : учеб. пособие / Н.А. Староверова, Э.П. Ибрагимова. — Электрон. дан. — Казань : КНИТУ, 2016. — 312 с

2.Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278.

3.Таненбаум Э. С., Бос Х. Современные операционные системы. Классика Computers Science. 4-е изд. г СПб.: Питер, 2018. – 1120с.

4.Ю.А.Родичев. Нормативная база и стандарты в области информационной безопасности. Учебное пособие - СПб.: Питер, 2017г. – 256стр.

5.Варлатая С.К., Шаханова М.В. Защита информационных процессов в компьютерных сетях. Учебно-методический комплекс. изд. Проспект, 2015. – 178с.

6.Скабцов Н. В. Аудит безопасности информационных систем. Изд. Питер, 2018. – 272стр.

7.В.Г. Олифер, Н.А. Олифер "Компьютерные сети. Принципы, технологии, протоколы". 5-е изд., – СПб: Питер, 2017.

8.Беленькая М.Н., Малиновский С.Т., Яковенко Н.В. Администрирование в информационных системах Учебное пособие для вузов 2-е изд., испр. и доп. – Москва: НТИ «Горячая линия–Телеком». – 2018; - 408стр.

9.Баранчиков А. И., Баранчиков П. А., Громов А. Ю., Ломтева О. А. Организация сетевого администрирования: Учебник. изд., Инфра-М, Форум, 2019 – 384 стр.

Дополнительные источники:

1.Аверченков, В.И. Криптографические методы защиты информации [Электронный ресурс] : учебное пособие / В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак. — Электрон. дан. — Москва : ФЛИНТА, 2017. — 215 с. — Режим доступа: https://e.lanbook.com/book/92914. — Загл. с экрана.

2.Уорд Б. Внутреннее устройство Linux. – СПб.: Питер, 2018. – 384 с.

3.Метрология, стандартизация, сертиф.,технич...: Уч. / В.Ю.Шишмарев-М.:КУРС, НИЦ ИНФРА-М,2018-312с(П) (ISBN 978-5-906923-15-8.

4.Операционные системы. Концепции построения и обеспечения безопасности Учебное пособие для вузов Мартемьянов Ю.Ф., Яковлев Ал.В., Яковлев Ан.В.2-е изд., стереотип. 2017г.

5.Организация и обеспечение безопасности информационно-технологических сетей и систем. Дмитрий Мельников Издательство: КДУ ISBN 978-5-98227-960-6, 978-5-4243-0004-2; 2015 г.

6.Анализ и диагностика компьютерных сетей Автор: Дж. Хогдал Издательство: Лори ISBN 978-5-85582-389-9; 2015 г.

Интернет-ресурсы:

Netacad.com

https://www.anti-malware.ru/

http://www.booksshare.net

### 4.3 Общие требования к организации образовательного процесса

Занятия проводятся спаренными уроками продолжительностью один академический час, общая продолжительность спаренного урока - 2 академических часа (1,5 астрономических часа). Образовательный процесс включает в себя проведение лекционных, комбинированных занятий, лабораторных работ, чередующихся друг с другом.

Учебная практика проводится концентрированно в лабораториях колледжа.

Реализация рабочей программы модуля должна обеспечиваться учебно методической документацией, доступом каждого обучающегося к базам данных и библиотечным фондам. Во время самостоятельной подготовки обучающиеся должны быть обеспечены доступом к сети Интернет.

Должны быть предусмотрены консультации в объеме не менее 0,5 часа в неделю по каждому МДК. Формы проведения консультаций: групповые, индивидуальные, письменные, устные.

Освоению данного модуля должно предшествовать изучение следующих дисциплин:

- ОП.01 Основы информационной безопасности;
- ОП.03 Организационно-правовое обеспечение информационной безопасности;
- ОП.04 Сети и системы передачи информации;
- ОП.07 Операционные систем;

### 4.4 Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарным курсам:

- наличие высшего профессионального образования, соответствующего профилю профессионального модуля «Эксплуатация подсистем безопасности автоматизированных систем».

- опыт деятельности в организациях соответствующей профессиональной сферы, эти преподаватели должны проходить стажировку в профильных организациях не реже 1 раза в 3 года.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой:

- дипломированные специалисты по профилю профессионального модуля;

- преподаватели междисциплинарных курсов.

## 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

| Результаты (освоенные профессиональные компетенции) | Основные показатели оценки результата | Формы и методы контроля и оценки |
|---|---|---|
| Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем. | Правильно выполняется ввод в эксплуатацию компонентов подсистем безопасности автоматизированных систем. | Защита лабораторных работ по темам 1-2 раздела 1МДК 01.01<br>Защита лабораторных работ по темам 1.1-3.2 МДК 01.02.<br>Защита курсового проекта.<br>Устные опросы по тематике прошедших лекций.<br>Возможен ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» КОД 1.1.и по компетенции Сетевое и системное администрирование КОД 1.1. |
| Участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности. | - Правильность проверки состояния и проведения технического обслуживания компонентов подсистем безопасности автоматизированных систем. Обнаружение и устранение неполадок в работе компонентов подсистем безопасности автоматизированных систем. | Защита лабораторных работ по темам 2-4 МДК 01.01<br>Защита лабораторных работ по темам 4.1-4.2 МДК 01.02<br>Защита курсового проекта.<br>Устные опросы по тематике прошедших лекций.<br>Возможен ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» КОД 1.1. и по компетенции Сетевое и системное администрирование КОД 1.1. |

| | | |
|---|---|---|
| Выполнять работы по администрированию подсистем безопасности автоматизированных систем. | Правильность конфигурирования подсистемы безопасности автоматизированных систем. | Наблюдение за выполнением и защита лабораторных работ по темам 5-10 МДК 01.01<br>Защита лабораторных работ по темам 5.1-11.2 МДК 02.02<br>Защита курсового проекта.<br>Дифференцированный зачет про учебной практике.<br>Устные опросы по тематике прошедших лекций.<br>Возможен ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» КОД 1.1. и по компетенции Сетевое и системное администрирование КОД 1.1. |
| Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них. | Правильное выполнение правил охраны труда и техники безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации. | Наблюдение за выполнением лабораторных работ и практической части курсового проекта.<br>Возможен ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» КОД 1.1. и по компетенции Сетевое и системное администрирование КОД 1.1. |
| Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах. | Ведение технической документации связанной с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах в соответствие с требованиями нормативно – технической документации | Возможен ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» КОД 1.1.<br>Возможен ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» КОД 1.1. и по компетенции Сетевое и системное администрирование КОД 1.1. |

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

| **Результаты (освоенные общие компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности. | Демонстрация интереса к будущей профессии. | *Наблюдение за выполнением и защита лабораторных работ, устные опросы по заданной тематике.*<br>*Выполнение курсового проекта.*<br>*Наблюдение за выполнением заданий по учебным практикам.* |
| Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество | -выбор и применение методов и способов решения профессиональных задач в области эксплуатации подсистем безопасности автоматизированных систем.<br>- правильность оценки эффективности и качества методов и способов решения профессиональных задач в области эксплуатации подсистем безопасности автоматизированных систем. | |
| Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность | Правильность эксплуатации подсистем безопасности автоматизированных систем и эксплуатации подсистем безопасности автоматизированных систем в стандартных и нестандартных ситуациях, нести ответственность за принятие решений в нестандартных ситуациях. | |
| Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития | Эффективный поиск информации для эксплуатации подсистем безопасности автоматизированных систем с использованием современных источников информации;<br>-эффективное использование информации для профессионального и личностного развития. | |
| Использовать информационно-коммуникационные технологии в профессиональной деятельности | Использование для эксплуатации подсистем безопасности автоматизированных систем и эксплуатации подсистем безопасности автоматизированных систем | |
| Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями | Взаимодействие с преподавателями, мастерами, обучающимися в ходе учебного процесса. | |

| | | |
|---|---|---|
| Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий | Ответственность за выполнение заданий, полученных группой студентов (группа не более двух человек) | |
| Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации | Организация самостоятельных занятий при изучении профессионального модуля;<br>-самоанализ и коррекция результатов собственной работы. | |
| Ориентироваться в условиях частой смены технологий в профессиональной деятельности. | Проявление интереса к инновациям в области эксплуатации подсистем безопасности автоматизированных систем. | *Посещение выставок, выполнение практических и лабораторных работ.* |
| Формулировать задачи логического характера и применять средства математической логики для их решения. | Использование математической логики, решение задач логического характера | *Наблюдение за выполнением лабораторных работ, курсового проекта, учебных практик* |
| Владеть основными методами и средствами разработки программного обеспечения. | Использование методов и средств разработки программного обеспечения | *Наблюдение за выполнением лабораторных работ* |
| Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах. | Правильное выполнение инсталляции и настройки АИС, регламентных работ в АИС | *Наблюдение за выполнением и защита лабораторных работ, курсового проекта, учебных практик* |