



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

Директор  /Н. Т. Бурганов/
« 30 »  2020г.

**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ**

**Основы работ на активном сетевом оборудовании и в современных
ОС с учетом стандартов Ворлдскиллс по компетенции
Кибербезопасность в дистанционном формате**

Категория слушателей: преподаватели

Уровень квалификации: 6

Объем: 36

Срок: 1 неделя

Форма обучения: очная с применением дистанционных форм

Организация обучения: непрерывно, по мере комплектования групп

Екатеринбург, 2020

Дополнительная профессиональная программа повышения квалификации Основы работ на активном сетевом оборудовании и в современных ОС с учетом стандартов Ворлдскиллс по компетенции Кибербезопасность в дистанционном формате предусматривает формирование у слушателей компетенций, позволяющих разрабатывать и развертывать комплексную информационную структуру предприятий, включающую рабочие станции, серверы и сетевое оборудование; организовывать защищенные соединения сетей предприятий.

Разработчики:

Уймин А.Г., преподаватель ГАПОУ СО УРТК им. А.С. Попова,
Терентьева О.А., руководитель профильного ресурсного центра робототехники
и информационных технологий ГАПОУ СО УРТК им. А.С. Попова,
Алферьева О.В., преподаватель ГАПОУ СО УРТК им. А.С. Попова

Оглавление

1.Общая характеристика программы	4
1.1 Нормативно-правовые основания разработки программы	4
1.2 Область применения программы	4
1.3 Требования к слушателям (категории слушателей)	4
1.4 Цель и планируемые результаты программы	5
1.5 Форма документа	5
2.Учебный план	6
3. Календарный учебный график	7
4.Содержание программы модулей	8
5.Организационно-педагогические условия реализации программы	9
5.1 Материально-техническое обеспечение	9
5.2 Информационное обеспечение программы	9
5.3 Организация образовательного процесса	9
5.4 Кадровое обеспечение образовательного процесса	10
6. Контроль и оценка результатов освоения программы	10

1.ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Нормативно-правовые основания разработки программы

Нормативно-правовую основу разработки программы составляют:

- Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденный приказом Минобрнауки России от 9 декабря 2016 г. N 1551;
- Техническое описание компетенции WSR «Кибербезопасность» 2020 года.

Программа разработана на основе профессиональных стандартов (квалификационных требований):

- Профессиональный стандарт 06.030 Специалист по защите информации в телекоммуникационных системах и сетях, утвержденного приказом Минтруда России от 03.11.2016 № 608Н.

1.2 Область применения программы

Настоящая программа предназначена для повышения квалификации преподавателей, осуществляющих подготовку обучающихся СПО по образовательной программе среднего профессионального образования по специальностям 10.02.03 Информационная безопасность автоматизированных систем, 10.02.02 Информационная безопасность телекоммуникационных систем, 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, 10.02.05 обеспечение информационной безопасности автоматизированных систем, а также подготовку обучающихся к участию в чемпионатах WSR по компетенции «Кибербезопасность».

1.3 Требования к слушателям (категории слушателей)

К освоению программы допускаются лица, имеющие среднее профессиональное или высшее образование в области информационных технологий и защиты информации. Слушатель должен обладать опытом администрирования информационно-коммуникационных систем (инфокоммуникационных систем) и обеспечением безопасности информационных систем и защиты информации. Требования к опыту работы и возрасту не установлены.

1.4 Цель и планируемые результаты освоения программы

Целью реализации программы является совершенствование следующих профессиональных компетенций:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 1	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты
ПК 2.1.	Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС.
ПК 2.2.	Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС и их диагностику, обнаружение отказов, формировать предложения по их устранению

1.5 Форма документа - по результатам освоения программы выдается удостоверение о повышении квалификации.

2 Учебный план

Наименование компонентов программы	Объем программы (академические часы)					
	Всего	Самостоятельная работа	Нагрузка во взаимодействии с преподавателем			
			Теоретическое обучение	Практическое и лабораторные работы	Практика (стажировка)	Промежуточная аттестация, форма
1	2	3	4	5	6	7
Модуль 1 Современные операционные системы семейства Linux и активное сетевое оборудование	20	-	4	16	-	-
Модуль 2 Конфигурация параметров безопасности и служб аутентификации на базе операционной системы Linux	10	-	2	8	-	-
Итого	30	-	6	24	-	-
Итоговая аттестация	6	-	-	-	-	Представление и защита проекта
Итого по программе	36	-	6	24	-	6

3. Календарный учебный график

Компоненты программы	Аудиторные занятия, час					Итоговая аттестация, час
	1 день	2 день	3 день	4 день	5 день	6 день
Раздел 1 Активное сетевое оборудование и современные ОС Семейства Linux	6	6	6	3		
Раздел 2 Выполнение работ по конфигурации параметров безопасности и служб аутентификации на базе ОС Linux				3	6	
Итоговая аттестация						6

4. Программы учебных модулей

Наименование модулей и тем программы	Содержание учебного материала, практические занятия, внеаудиторная (самостоятельная) учебная работа слушателей		Объём
<i>1</i>	<i>2</i>		<i>3</i>
Раздел 1 Современные операционные системы семейства Linux и активное сетевое оборудование			
Тема 1.1 Настройка и конфигурация сетевого оборудования и служб Настройка механизмов безопасности	Содержание	Уровень освоения	4
	Активное сетевое оборудование и современные ОС Семейства Linux. Проблемы обеспечения безопасности операционных систем Архитектура подсистемы защиты операционной системы семейства Linux.	3	
	Практические занятия		16
	1. Настройка подключений к глобальным сетям на активном сетевом оборудовании 2. Настройка маршрутизации 3. Настройка механизмов безопасности 4. Настройка параметров мониторинга и резервного копирования 5. Конфигурация хостов на базе ОС Linux 6. Конфигурация служб удаленного доступа на базе ОС Linux		
	Самостоятельная работа		
Промежуточная аттестация в форме (зачета, экзамена)			0
Раздел 2 Конфигурация параметров безопасности и служб аутентификации на базе операционной системы Linux			
Тема 2.1 Выполнение работ по конфигурации параметров безопасности. Службы аутентификации на базе ОС Linux	Содержание	Уровень освоения	2

	Концепция адаптивного управления безопасностью. Технология анализа защищенности. Параметры безопасности. Службы аутентификации	3	
	Практические занятия		8
	1.Выполнение работ по конфигурации параметров безопасности 2.Выполнение работ по конфигурации служб аутентификации на базе ОС Linux 3. Выполнение работ по конфигурации служб централизованного управления и журналирования на базе ОС Linux		
Итоговая аттестация	Представление и защита проекта «Обеспечение безопасности операционных систем семейства Linux»		6
Итого			36

5. Организационно-педагогические условия реализации программы

5.1. Материально-техническое обеспечение

Реализация программы предполагает наличие мастерской по кибербезопасности.

Оборудование одного учебного места требует:

- ПЭВМ в сборе (i7/32Gb MEM/ 256Gb + 1Tb nvme SSD/ Nvidia Quadro 1000 / Intel 4x1Gb/s Lan Card/ 27” Monitor)
- Сервер виртуализации для центральной инфраструктуры (домен, генератор трафика)
- Виртуальная машина
- Виртуальная машина (контроллер домена)
- Виртуальная машина (сервер)
- Виртуальная машина (клиент)
- Коммутатор
- Маршрутизатор или аналог на виртуальной машине
- Источник бесперебойного питания
- Точка доступа или возможность создания WiFi сетей

Технические средства обучения:

- Проектор Epson EB-2247U;
- Экран для проектора Lumien Master Picture 191x300 Matte White FiberGlass.

5.2. Информационное обеспечение обучения

Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

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

2. Бутакова, Н.Г. Криптографические методы защиты информации, учебное пособие [Электронный ресурс] : учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. — Электрон. дан. — Санкт-Петербург : ИЦ Интермедия, 2016. — 384 с. — Режим доступа: <https://e.lanbook.com/book/90270>. — Загл. с экрана.

3. Стеганографические и криптографические методы защиты информации: учебное пособие [Электронный ресурс] : учеб. пособие — Электрон. дан. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Режим доступа: <https://e.lanbook.com/book/90963>. — Загл. с экрана.

4. Лидовский, В.В. Основы теории информации и криптографии [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : , 2016. — 141 с. — Режим доступа: <https://e.lanbook.com/book/100349>

Дополнительные источники:

1. Ю.А.Родичев. Нормативная база и стандарты в области информационной безопасности. Учебное пособие - СПб.: Питер, 2017г. – 256 стр.
2. Бутакова, Н.Г. Криптографические методы защиты информации, учебное пособие [Электронный ресурс] : учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. — Электрон. дан. — Санкт-Петербург : ИЦ Интермедия, 2016. — 384 с. — Режим доступа: <https://e.lanbook.com/book/90270>. — Загл. с экрана.
3. Стеганографические и криптографические методы защиты информации: учебное пособие [Электронный ресурс] : учеб. пособие — Электрон. дан. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Режим доступа: <https://e.lanbook.com/book/90963>. — Загл. с экрана.
4. Лидовский, В.В. Основы теории информации и криптографии [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : , 2016. — 141 с. — Режим доступа: <https://e.lanbook.com/book/100349>

Интернет-ресурсы:

- 1.<http://cryptogrof.ru/>

5.3. Организация образовательного процесса

Предусмотрены следующие виды учебных занятий: (перечисляются виды занятий, применяемые технологии, организация консультаций и пр.).

- лекция с элементами беседы – объяснение теоретических основ;
- практические занятия – совершенствование навыков работы при решении алгоритмических задач;
- итоговая аттестация – представление и защита проекта «Обеспечение безопасности операционных систем семейства Linux»

5.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров:

Наличие среднего профессионального или высшего образования в области информационных технологий, опыт работы по направлению корпоративная защита от внутренних угроз информационной безопасности и кибербезопасность, опыт подготовки обучающихся к участию в чемпионатах WSR по направлению «Информационная безопасность».

6. Контроль и оценка результатов освоения программы

6.1. К итоговой аттестации допускаются слушатели, успешно прошедшие промежуточный контроль предусмотренный учебным планом настоящей программы.

К итоговой аттестации слушатели представляют следующие материалы: презентация разработанного проекта.

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата
Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС.	Установка (монтаж), настройка (наладка) и запуск в эксплуатацию программно-аппаратных средств обеспечения информационной безопасности ИТКС осуществлены в соответствии с техническим заданием.
Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС и их диагностику, обнаружение отказов, формировать предложения по их устранению	Обеспечена эксплуатация и содержание в работоспособном состоянии программно-аппаратных средств обеспечения информационной безопасности ИТКС и их диагностика.