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

Утверждаю
Директор _____ /Н. Т. Бурганов/
«_02_» _7 сентября_ 2020г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Развитие образовательного процесса на основе освоения педагогом профессионального обучения современных производственных технологий

Категория слушателей: преподаватели

Уровень квалификации: 6

Объем: 36

Срок: 1 неделя

Форма обучения: очная

Организация обучения: непрерывно, по мере комплектования групп

Екатеринбург, 2020

Дополнительная профессиональная программа повышения квалификации «Развитие образовательного процесса на основе освоения педагогом профессионального обучения современных производственных технологий». Курс предусматривает освоение современных производственных технологий предприятий и организаций, включая установку и конфигурирование безопасной работы информационной системы как основу обеспечения производственного цикла.

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

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 2	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты
ПК 2.1.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях
ПК 2.3.	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями

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	Практические и лабораторные работы	Практика (стажировка)	Промежуточная аттестация, форма
1	**2**	**3**	**4**	**5**	**6**	7
Модуль 1 Безопасная конфигурация программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей	20	-	4	16	-	-
Модуль 2 Поддержка бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях	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 Безопасная конфигурация программных и программно-аппаратных средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей	6	6	6	3		
Раздел 2 Выполнение работ по защите информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств				3	6	
Итоговая аттестация						6

4. Программы учебных модулей

Наименование модулей и тем программы	Содержание учебного материала, практические занятия, внеаудиторная (самостоятельная) учебная работа слушателей		Об ъе
1	*2*		*3*
Раздел 1 Безопасная конфигурация программных и программно-аппаратных средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей			
Тема 1.1 Обеспечение безопасной конфигурации программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей	**Содержание**	**Уровень освоения**	4
	Повышение защищенности и отказоустойчивости операционной системы, веб-сервера, сервера баз данных, другого программного обеспечения. Повышение безопасности при установке и конфигурировании безопасной работы информационной системы (веб сайта с базой данных) и анализ его программного кода, поиск уязвимостей и угроз. Поиск и устранение найденных недостатков с точки зрения повышения безопасности отдельных функций веб сайта	3	
	Практические занятия		16
	1. Настройка операционной системы, веб-сервера, сервера баз данных для повышения защищенности и отказоустойчивости системы 2. Установка и конфигурирование безопасной работы информационной системы (веб сайта с базой данных) 3. Анализ программного кода, поиск уязвимостей и угроз веб сайту с базой данных 4. Доработка и устранение найденных недостатков и рефакторинг программного кода с точки зрения повышения безопасности отдельных функций веб сайта		
	Самостоятельная работа		0
	Промежуточная аттестация в форме (**зачета, экзамена**)		0
Раздел 2 Выполнение работ по защите информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств			

Тема 2.1 Выполнение работ по защите информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств	**Содержание**	**Уровень освоения**	2
	Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Концепция построения виртуальных защищенных сетей. Надежная передача информации по незащищенным каналам связи. Шифрование.	3	
	Практические занятия		8
	1. Настройка и применение средств защиты информации в операционных системах, в том числе средства антивирусной защиты 2. Осуществление установки и настройки программных и программно-аппаратных, в том числе криптографических средств защиты информации 3. Осуществление восстановления процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации		
Итоговая аттестация	Представление и защита проекта «Безопасная конфигурация»		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 Qadro 1000 / Intel 4x1Gb/s Lan Card/ 27” Monitor)
- Сервер виртуализации для центральной инфраструктуры (домен, генератор трафика)
- Виртуальная машина (сервер DLP)
- 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 «Безопасная конфигурация»

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**
Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей	Правильное применение технологий осуществления установки, настройки и запуска в эксплуатацию программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей
Поддерживать бесперебойную работу программных и программно-аппаратных,	Штатно функционирующие программные и программно-

в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях	аппаратные, в том числе криптографические средства защиты информации
Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями	Штатно функционирующий информационный ресурс в максимально безопасном окружении