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

Утверждаю
Директор _____ /Н. Т. Бурганов/
«07» сентября 2020г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Использование инновационных производственных технологий в образовательной деятельности профессиональной образовательной организации (с учетом стандартов Ворлдскиллс по компетенции Корпоративная защита от внутренних угроз информационной безопасности)

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 «Использование инновационных производственных технологий в образовательной деятельности профессиональной образовательной организации (с учетом стандартов Ворлдскиллс по компетенции Корпоративная защита от внутренних угроз информационной безопасности). Курс предусматривает изучение требований к условиям, оборудованию, технологической оснастке при освоении инновационных производственных технологий по специальностям направления информационной безопасности, освоению технологий работы на инновационном оборудовании для обеспечения корпоративной защиты от внутренних угроз информационной безопасности.

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 «Корпоративная защита от внутренних угроз информационной безопасности» 2019 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 «Корпоративная защита от внутренних угроз информационной безопасности».

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
ПК 2.3.	Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС

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 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств	20	-	4	16	-	-
Модуль 2 Выполнение работ по защите информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств	10	-	2	8	-	-
Итого	**30**	-	6	24	-	-
Итоговая аттестация	6	-	-	-	-	Представление и защита проекта «Защита информации в ИС»
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 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств	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 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств			
Тема 1.1 Обеспечение безопасности операционных систем и технология разграничения доступа. Основы технологии виртуальных защищенных сетей VPN	**Содержание**	**Уровень освоения**	
	Проблемы обеспечения безопасности операционных систем Архитектура подсистемы защиты операционной системы Windows. Технологии виртуальных защищенных сетей VPN Server2016	3	4
	Практические занятия		16
	1. Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав пользователя 2. Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита 3. Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация 4. Программы надежного удаления информации 5. Программные средства резервного копирования. Настройка RAID-массивов 6. Изучение основных возможностей ПО VipNetClient		
	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 Защита 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. Модель ISO/OSI и стек протоколов TCP/IP. Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях. Концепция построения виртуальных защищенных сетей. Надежная передача информации по незащищенным каналам связи. Шифрование.	3	
	Практические занятия		8
	1. Основные действия с виртуальной машиной. Работа с контрольными точками 2.Использование внешних устройств. Работа с локальным хранилищем сертификатов в ОС WINDOWS 3.Установка и настройка ПО eTokenPKIClient. Настройка ПО eTokenPKIClient с помощью групповых политик 4.Развертывание и настройка TMS в среде Active Directory 5.Настройка политик и использования виртуального токена. Использование токена на рабочем месте администратора 6.Установка и настройка СКЗИ «КриптоПроCSP».		
Итоговая аттестация	Представление и защита проекта «Защита информации в ИС»		6
Итого			**36**

5. Организационно-педагогические условия реализации программы

5.1.Материально-техническое обеспечение

Реализация программы предполагает наличие компьютерного класса – мастерской по сетевому и системному администрированию.

Оборудование одного учебного места требует:

- Ноутбук или ПК в сборе
- Монитор
- 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;
- экран.

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 «Защита информации в ИС»

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 безопасностьи».

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.	Правильное применение технологий осуществления установки (монтаж), настройки (наладку) и запуска в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС
Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств	Выявление и оценивание угрозы безопасности информации в ИТКС; производство контроля показателей и процесса

обеспечения информационной безопасности ИТКС и их диагностику, обнаружение отказов, формировать предложения по их устранению	функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации.
Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС	Правильное формулирование предложений по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС при выявлении и оценивании угрозы безопасности информации в ИТКС