Министерство образования Пензенской области
Государственное автономное профессиональное
образовательное учреждение Пензенской области
«Пензенский колледж информационных и промышленных технологий (ИТ-колледж)»
(ГАПОУ ПО ПКИПТ (ИТ-колледж))

УТВЕРЖДАЮ
Директор ГАПОУ ПО «Пензенский колледж информационных и промышленных технологий (ИТ-колледж)».
_____А.Н. Фетисов
«_31_» _октября_ 2019г.

.

Дополнительная профессиональная программа повышения квалификации

«Защита информации от внутренних и внешних угроз с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

Пенза, 2019г.

Дополнительная профессиональная программа повышения квалификации «Защита информации от внутренних и внешних угроз с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

разработана с учетом требований:

- федерального государственного образовательного стандарта среднего профессионального образования (ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем), квалификации «Техник по защите информации»;
- стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»;
- профессионального стандарта "Консультант в области развития цифровой грамотности населения (цифровой куратор)";
- профессионального стандарта № 16199 «Оператор электронно-вычислительных и вычислительных машин».

Организация – разработчик: ГАПОУ ПО «Пензенский колледж информационных и промышленных технологий (ИТ-колледж)»

Разработчики

_____ Сазонова А.Ю. преподаватель ГАПОУ ПО ПКИПТ

_____ Пузренков А.Н., преподаватель ГАПОУ ПО ПКИПТ

Дополнительная профессиональная программа повышения квалификации «Защита информации от внутренних и внешних угроз с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» одобрена МЦК профессиональных дисциплин по УГС 10.00.00 Информационная безопасность

Протокол №_3_ от _31_ _10_ 2019г.

Председатель МЦК _____ (подпись) Сазонова А.Ю.

СОГЛАСОВАНО

Заместитель директора по научно-методической работе, доктор педагогических наук _____ В.Н. Корчагин

Заместитель директора по работе с социальными партнерами _____ Н.В. Чистякова

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Пояснительная записка

Программа повышения квалификации «Защита информации от внутренних и внешних угроз с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» разработана на основе Федерального государственного образовательного стандарта (ФГОС), имеет «направленность (профиль) образования - ориентированный на конкретные виды деятельности, определяющие ее предметно-тематическое содержание, преобладающие виды учебной деятельности обучающегося и требования к результатам освоения образовательной программы» (Федеральный закон Российской Федерации «Об образовании в РФ» (от 29.12.12г.№273-ФЗ).

Цель программы: Дополнительная профессиональная программа повышения квалификации направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации, с учетом спецификации стандарта Ворлскиллс по компетенции **«Корпоративная защита от внутренних угроз информационной безопасности»**; изучение дополнительных вопросов, связанных с использованием правовых и программных средств для решения прикладных задач информационной безопасности, совершенствование знаний и умений обучающихся в сфере информационной безопасности.

1.2. Планируемые результаты обучения

1.2.1. В результате освоения программы повышения квалификации «Защита информации от внутренних и внешних угроз с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» слушатель должен **знать**:

- Правовые основы защиты информации
- Организационные основы защиты информации
- Физические основы защиты информации
- Основные каналы утечек данных
- Историю и основы криптографии
- Историю и основы стеганографии
- Виды сетевых атак и защиту

1.2.2. В результате освоения программы повышения квалификации «Защита информации от внутренних и внешних угроз с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» слушатель должен **уметь:**

- - установить системы виртуализации;
- - настроить программы виртуализации под необходимые требования;
- - устанавливать серверные ОС семейства Windiws;
- - устанавливать серверные ОС семейства linux;
- - произвести настройку серверных ОС семейства Windows;

- - произвести настройку серверных ОС семейства linux;
- - произвести установку системы DLP;
- - настроить политики безопасности работы в сети;
- - настроить политики безопасности работы с физическими устройствами;
- - контроль пользователей;
- - выявлять и расследовать инциденты информационной безопасности.

1.3. Трудоемкость обучения: 40 часов

1.4. Форма обучения: очно-заочная

1.5. График занятий

1 неделя	2 неделя	3 неделя	4 неделя	5 неделя	6 неделя	7 неделя	8 неделя
6 часов	6 часов	6 часов	6 часов	4 часа	4 часа	4 часа	4 часа

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Рабочий учебный план

Министерство образования Пензенской области
Государственное автономное профессиональное образовательное учреждение
Пензенской области
«Пензенский колледж информационных и промышленных технологий (ИТ-колледж)»
(ГАПОУ ПО ПКИПТ)

УТВЕРЖДАЮ
Директор ГАПОУ ПО ПКИПТ
_____ А.Н. Фетисов
«31» октября 2019 г.

РАБОЧИЙ УЧЕБНЫЙ ПЛАН
Дополнительной профессиональной программы повышения квалификации «Защита информации от внутренних и внешних угроз с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

Категория слушателей лица, имеющие или получающие среднее профессиональное и высшее образование

Трудоемкость обучения (всего) 40 часов

Срок обучения 2 месяца

Форма обучения очно-заочная

№ п/п	Наименование учебных дисциплин	Формы аттестации			Учебная нагрузка слушателя, час.				
		Экзамен	Зачет	Контрольная работа	Максимальная	Самостоятельная	Обязательная		
							Всего	в том числе	
								теоретическое обучение дистанционно	лабораторные и практические занятия
1.	Ознакомление с WSI и Ворлдскиллс Россия. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации				12	4	8	8	
2.	Правовые основы защиты информации				6	2	4	2	2

3.	Организационные основы защиты информации				**12**	**4**	**8**	**2**	**6**
4.	Физические основы защиты информации				**9**	**3**	**6**	**4**	**2**
5.	Основные каналы утечек данных				**15**	**5**	**10**	**2**	**8**
6.	Криптография и стеганография				**6**	**2**	**4**	**2**	**2**
	Итого		**1**		**60**	**20**	**40**	**20**	**20**

Согласовано

Заместитель директора по работе с социальными партнерами _____ Чистякова Н.В.
(подпись)

Председатель цикловой методической комиссии _____ Сазонова А.Ю,
(подпись)

2.2. Дисциплинарное содержание программы

«Защита информации от внутренних и внешних угроз с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

2.2.1. Тематический план учебной дисциплины«Защита информации от внутренних и внешних угроз с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

№	Наименование темы	Количество часов, в том числе				
		Максимальная учебная нагрузка слушателя, час.	Аудиторные занятия			Самостоятельная дистанционная работа
			Теоретические занятия дистанционно	Практические занятия	Лабораторные занятия	
1	2	3	4	5	6	7
	Ознакомление с WSI и Ворлдскиллс Россия. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации	**12**	**8**			**4**
	История, современное состояние и перспективы движения WorldSkills International (WSI) и Ворлдскиллс Россия («Молодые профессионалы») как инструмента развития профессиональных сообществ и систем подготовки кадров	6	4			2
	Актуальное техническое описание по компетенции. Спецификация стандарта Ворлдскиллс по компетенции **«Корпоративная защита от внутренних угроз информационной безопасности»**	6	4			2
	Правовые и организационные основы защиты информации	**6**	**2**	**2**	**0**	**2**
	Правовые основы защиты информации	3	2			1
	Организационные и физические основы защиты информации	3		2		1
	Защита каналов связи	**12**	**2**	**6**	**0**	**4**
	Основные каналы утечек данных	3	2			1
	Акустические каналы утечек данных	3		2		1
	Виброакустические каналы утечек данных	3		2		1
	Электромагнитные каналы утечек данных	3		2		1
	Криптографические методы защиты информации	**9**	**4**	**2**	**0**	**3**
	История криптографии	3	2			1
	Современная криптография	3	2			1
	Хэши	3		2		1
	Стеганографические методы защиты информации	**15**	**2**	**8**	**0**	**5**
	История стеганографии	3	2			1
	Электронная стеганография	3		2		1

	Цифровая стеганография	3		2		1
	Шестнадцатиричный код	3		2		1
	Атаки на стегосистемы	3		2		1
	Виды сетевых атак	**6**	**2**	**2**	**0**	**2**
	Основные виды сетевых атак	4	2			2
	Зачетная работа	2		2		
	Итого	**60**	**12**	**20**	**0**	**16**

2.2.2. Рабочая программа учебной дисциплины «Защита информации от внутренних и внешних угроз с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

Раздел 1 Устройство компьютера

Тема 1.1. Ознакомление с WSI и Ворлдскиллс Россия. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации

Ознакомление с WSI и Ворлдскиллс Россия. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации.

Практическое занятие №1 Ознакомление с WSI и Ворлдскиллс Россия

Ознакомление с WSI и Ворлдскиллс Россия.

Тема 1.2. История, современное состояние и перспективы движения WorldSkills International (WSI) и Ворлдскиллс Россия («Молодые профессионалы») как инструмента развития профессиональных сообществ и систем подготовки кадров

История, современное состояние и перспективы движения WorldSkills International (WSI) и Ворлдскиллс Россия («Молодые профессионалы») как инструмента развития профессиональных сообществ и систем подготовки кадров.

Практическое занятие №2 История, современное состояние и перспективы движения WorldSkills International (WSI)

История, современное состояние и перспективы движения WorldSkills International (WSI) и Ворлдскиллс Россия («Молодые профессионалы») как инструмента развития профессиональных сообществ и систем подготовки кадров.

Тема 1.3. Актуальное техническое описание по компетенции. Спецификация стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

Актуальное техническое описание по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

Практическое занятие №3 Актуальное техническое описание по компетенции. Спецификация стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

Актуальное техническое описание по компетенции. Спецификация стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

Тема 1.4. Правовые и организационные основы защиты информации

Законы, регулирующие защиту информации. Организация защиты информации

Практическое занятие №4 Правовые и организационные основы защиты информации

Поиск законов по защите информации. Разработка организационных норм по защите информации

Тема 1.5. Правовые основы защиты информации

Практическое занятие №5 Правовые основы защиты информации

Характерные особенности правовых основ защиты информации.

Тема 1.6. Организационные и физические основы защиты информации.

Практическое занятие №6 Организационные и физические основы защиты информации.

Характеристики организационных и физических основ защиты информации.

Тема 1.7. Защита каналов связи

Типы каналов связи. Основы защиты каналов связи

Практическое занятие №7 Защита каналов связи

Конструктивные особенности защиты каналов связи.

Тема 1.8. Основные каналы утечек данных.

Основные каналы утечек данных. Акустические каналы утечек данных. Виброакустические каналы утечек данных. Электромагнитные каналы утечек данных.

Практическое занятие №8 Основные каналы утечек данных.

Конструктивные особенности основных каналов утечек данных.

Раздел 2 Способы безопасной передачи информации

Тема 2.1. Криптографические методы защиты информации

Практическое занятие №9 Криптографические методы защиты информации.

Методы шифрования данных.

Тема 2.2. История криптографии.

Практическое занятие №10 История криптографии.

История безопасных способов передачи информации.

Тема 2.3. Современная криптография.

Практическое занятие №11 Работа с программными средствами по шифрованию данных.

Принципы шифрования и работы программ по шифрованию. Хеши

Раздел 3 Стеганография

Тема 3.1. Стеганографические методы защиты информации

Теоритические основы стеганографии. Принцип работы стеганографических программ

Практическое занятие №12 Стеганографические методы защиты информации
Особенности применения стеганографических программ.

Тема 3.2. История стеганографии.
Практическое занятие №13 История стеганографии.
Особенности применения исторических методов стеганографии.

Тема 3.3. Электронная и цифровая стеганография.
Практическое занятие №14 Цифровые водяные знаки.
Особенности применения цифровых водяных знаков. Цифровая стеганография. Шестнадцатиричный код.

Раздел 4 Виды сетевых атак
Тема 4.1. Виды сетевых атак
Изучение основных видов сетевых атак
Практическое занятие №15 Виды сетевых атак
Изучение на виртуальных стендах сетевых атак.

Раздел 5 Криптоанализ и стегоанализ
Тема 5.1. Выявление стегоконтейнеров и расшифровка сообщений
Методики выявления и дешифровки криптографии и стеганографии.
Практическое занятие №16 Криптоанализ и стегоанализ
Произвести анализ шифров и стегоконтейнеров.

III. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по теоретическому обучению: обеспечивается педагогическими кадрами, имеющими высшее образование, соответствующее профилю преподаваемой дисциплины, а также имеющими документ на право проведения регионального чемпионата Ворлдскиллс Россия, оценивания демонстрационного экзамена по стандартам Ворлдскиллс Россия.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: мастера производственного обучения и преподаватели, имеющие высшее техническое профессиональное образование по профилю подготовки с квалификацией первой и высшей категории.

3.2. Информационно – методические условия реализации программы

Наименование учебной дисциплины	Перечень литературы, Интернет - ресурсов
Защита информации от внутренних и внешних угроз	1. Секреты информационной безопасности/А.И. Гладких. – М: Альпина Паблишерз, 2018 2. https://www.securitylab.ru/ 3. https://inatack.ru/ 4. https://xacker.ru/

3.3. Материально-технические условия реализации программы

Приведение сведений об условиях проведения лекций, лабораторных и практических занятий, а также об используемом оборудовании и информационных технологиях:

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Кабинет корпоративной защиты от внутренних угроз информационной безопасности	Лекции, практические занятия	- рабочие места по количеству обучающихся (в том числе оборудованные); - наглядные пособия, раздаточный материал; - видеотека по курсу; - учебные фильмы(частотный анализ, ххх, виды атак, учет подключенных устройств) по некоторым разделам дисциплины; - учебные наглядные пособия; - проектор, доска для проектора. **Оборудование и технологическое**

		оснащение рабочих мест: - натуральные образцы, применяемый инструмент и приспособления, технологическая документация. **Одно рабочее место должно содержать:** - персональный компьютер подключенныq к сети Internet; - программное обеспечение для проведения необходимых работ; - ОС для установки; - система виртуализации; - набор принадлежностей и расходных материалов; - флеш-карты; - ноутбук, подключенный к сети internet; - пакет антивирусной защиты.

IV. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

4.1. Формы аттестации: зачет

4.2. Оценочные материалы

Теоретические вопросы к зачету:

Теоретические вопросы к зачету:

1. Кодекс этики WS?
2. История движения WS?
3. Правовые особенности защиты информации?
4. Защита каналов связи?
5. Основные каналы утечек данных?
6. История криптографии.
7. Что такое хэш? Особенности применения.
8. Что такое стеганография?
9. Отличия стеганографии от криптографии?
10. Особенности использования электронной стеганографии?
11. Атаки на стегосистемы?
12. Что такое шестнадцатиричный код?
13. Виды сетевых атак?
14. Особенности проведения криптоанализа?
15. Особенности проведения стегоанализа?

Практические задания

1. Произвести защиту речевого канала связи.
2. Произвести шифрование сообщения любым доступным методом.
3. Произвести криптоанализ сообщения.
4. Произвести внедрение сообщения в различные файлы-контейнеры.
5. Произвести ручное внедрение сообщения в файл-контейнер.
7. Произвести стегоанализ.

8. Записать сообщение в шестнадцатиричный код различных файлов.
9. Выполнить сетевые атаки на виртуальных стендах.