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
«29» 11 2019г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

«Организация обработки и защиты персональных данных»

Пенза – 2019

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

Разработчики: Д.А. Ручкин, преподаватель первой категории

Дополнительная общеразвивающая программа рассмотрена на заседании МЦК профессиональных дисциплин по укрупненной группе специальности 10.00.00 «Информационная безопасность»

Протокол № 3 от 05.11.19 г.

Председатель МЦК _____ А.Ю. Сазонова

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель программы: Формирование знаний и навыков, необходимых для организации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов, органов местного самоуправления и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

1.2. Образовательные результаты программы

В результате освоения программы слушатель должен **уметь**:

- создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных;
- планировать мероприятия по обеспечению безопасности персональных данных;
- обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;
- проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных.

В результате освоения программы слушатель должен **знать**:

- основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;
- основные виды угроз безопасности персональных данных в информационных системах персональных данных; содержание и порядок организации работ по выявлению угроз безопасности персональных данных;
- процедуры задания и реализации требований по защите информации в информационных системах персональных данных;
- меры обеспечения безопасности персональных данных;
- требования по обеспечению безопасности персональных данных;
- порядок применения организационных мер и технических средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

1.3. Трудоемкость обучения: 72 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 (ИТ-колледж))

УТВЕРЖДАЮ
Директор ГАПОУ ПО ПКИПТ
_____А.Н. Фетисов
«25» 11 2019г.

РАБОЧИЙ УЧЕБНЫЙ ПЛАН
дополнительной общеразвивающей программы

«Организация обработки и защиты персональных данных»

Категория слушателей

- граждане, субъекты персональных данных
- операторы ПДн, специалисты организаций;
- юристы, специалисты правовой сферы;
- разработчики информационных систем, специалисты в области реализации автоматизированных решений;

Трудоемкость обучения 72 часа
Срок обучения 2 недели
Форма обучения очно-заочная

№	Наименование модулей	Всего, ак. час	В том числе			Форма контроля
			лекции	практ. занятия	промеж. и итог. контроль	
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Основы законодательства в области защиты персональных данных. Права субъекта ПДн и обязанности оператора. Особенности обработки персональных данных без использования средств автоматизации.	16	8	8	0	-
2	Основные этапы обработки и защиты персональных данных. Анализ объекта информатизации. Составление модели угроз.	16	8	8	0	-
3	Техническое задание на систему защиты ПДн.	8	4	4	0	-
4	Стадия проектирования. Требования методических документов. Стадия ввода в действие и эксплуатации СЗПДн.	12	4	8	0	-
5	Особенности защиты персональных	20	10	10	0	-

	данных при их обработке в государственных информационных системах. Контроль в области защиты персональных данных.					
ИТОГО:		**72**	**34**	**38**	**0**	**-**

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

Председатель методической цикловой комиссии _____ А.Ю. Сазонова

2.2. Содержание программы

2.2.1. Тематический план дополнительной общеразвивающей программы «Организация обработки и защиты персональных данных»

№	Наименование модулей	Всего, ак. час	В том числе			Форма контроля
			лекции	практ. занятия	промеж. и итог. контроль	
1	*2*	*3*	*4*	*5*	*1*	*2*
1	**Основы законодательства в области защиты персональных данных. Права субъекта ПДн и обязанности оператора. Особенности обработки персональных данных без использования средств автоматизации.**	**16**	**8**	**8**	**0**	**-**
1.1	Анализ международного и Российского законодательства по вопросам обработки ПДн и обеспечения безопасности ПДн.	4	4			
1.2	Особенности обработки персональных данных, осуществляемой без использования средств автоматизации	4	4			
1.3	Работа в программе Консультант Плюс. Поиск правовых документов в программе Консультант Плюс. Изучение ФЗ № 152-ФЗ «О персональных данных». Изучение Постановление Правительства РФ от 15.09.2008 № 687. Разработка Положения об обработке персональных данных сотрудников организации	8		8		
2	**Основные этапы обработки и защиты персональных данных. Анализ объекта информатизации. Составление модели угроз.**	**16**	**8**	**8**	**0**	**-**
2.1	Состав мероприятий по приведению информационных систем и процессов обработки персональных данных в соответствие с требованиями законодательства	4	4			
2.2	Стадия предпроектного обследования	4	4			
2.3	Разработка модели угроз и модели нарушителя организации. Изучение Постановление правительства РФ от 01.11.2012 г. № 1119.	8		8		
3	**Техническое задание на систему защиты ПДн.**	**8**	**4**	**4**	**0**	**-**
3.1	Составление частного технического задания на разработку системы защиты персональных данных. Обоснование разработки системы защиты ПДн.	4	4			
3.2	Изучение Приказа ФСТЭК России от	4		4		

	18.02.2013 г. № 21, Приказа ФСБ России от 10.07.2014 г. № 378.					
4	**Стадия проектирования. Требования методических документов. Стадия ввода в действие и эксплуатации СЗПДн.**	**12**	**4**	**8**	**0**	**-**
4.1	Этап внедрения. Обучение персонала.		2			
4.2	Разработка системы защиты ПДн.		2			
4.3	Программно-технические комплексы защиты информации от несанкционированного доступа. Технические средства перекрытия технических каналов утечки информации.			8		
5	**Особенности защиты персональных данных при их обработке в государственных информационных системах. Контроль в области защиты персональных данных.**	**20**	**10**	**10**	**0**	**-**
5.1	Регуляторы в области защиты персональных данных.		6			
5.2	Особенности защиты персональных данных при их обработке в государственных информационных системах.		4			
5.3	Подготовка объекта к аттестации. Типовые формы документов. Изучение методов обезличивания персональных данных.			10		
ИТОГО:						

2.2.1.1. Содержание дополнительной общеразвивающей программы «Организация обработки и защиты персональных данных»

Тема 1 Основы законодательства в области защиты персональных данных. Права субъекта ПДн и обязанности оператора. Особенности обработки персональных данных без использования средств автоматизации.

Анализ международного и Российского законодательства по вопросам обработки ПДн и обеспечения безопасности ПДн. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Права субъекта персональных данных, обязанности оператора.

Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Постановление Правительства РФ от 15.09.2008 № 687.

Практические работы.

Работа в программе Консультант Плюс. Поиск правовых документов в программе Консультант Плюс. Изучение ФЗ № 152-ФЗ «О персональных данных».

Изучение Постановление Правительства РФ от 15.09.2008 № 687. Разработка Положения об обработке персональных данных сотрудников организации.

Тема 2 Основные этапы обработки и защиты персональных данных. Анализ объекта информатизации. Составление модели угроз.

Состав мероприятий по приведению информационных систем и процессов обработки персональных данных в соответствие с требованиями законодательства о персональных данных. Постановление правительства РФ от 01.11.2012 г. № 1119.

Стадия предпроектного обследования. Составление перечня ПДн, перечня сотрудников, работающих с ПДн. Описание ИСПДн. Выявление угроз безопасности персональных данных при их обработке в ИСПДн. Разработка частной модели угроз безопасности ПДн. Базовая модель угроз безопасности ПДн при их обработке в ИСПДн. Определение актуальности угроз в соответствии с методическими документами ФСТЭК России. Разработка модели нарушителя.

Практические работы.

Разработка модели угроз и модели нарушителя организации.

Изучение Постановление правительства РФ от 01.11.2012 г. № 1119.

Тема 3 Техническое задание на систему защиты ПДн.

Составление частного технического задания на разработку системы защиты персональных данных. Обоснование разработки системы защиты ПДн. Требования методических документов ФСТЭК и ФСБ России к составу и содержанию организационных и технических мер по обеспечению безопасности ПДн. Приказ ФСТЭК России от 18.02.2013 г. № 21, Приказ ФСБ России от 10.07.2014 г. № 378.

Практические работы.

Изучение Приказа ФСТЭК России от 18.02.2013 г. № 21, Приказа ФСБ России от 10.07.2014 г. № 378.

Тема 4 Стадия проектирования. Требования методических документов. Стадия ввода в действие и эксплуатации СЗПДн.

Этап внедрения. Обучение персонала. Установка, настройка, учет и контроль СЗИ. Описание системы защиты персональных данных. Проверка эффективности СЗПДн.

Разработка системы защиты ПДн. Выбор средств защиты информации. Организационные мероприятия.

Практические работы.

Программно-технические комплексы защиты информации от несанкционированного доступа. Технические средства перекрытия технических каналов утечки информации.

Тема 5 Особенности защиты персональных данных при их обработке в государственных информационных системах. Контроль в области защиты персональных данных.

Регуляторы в области защиты персональных данных. Проверки Роскомнадзора. Проверки ФСБ. Проверка ФСТЭК.

Особенности защиты персональных данных при их обработке в государственных информационных системах.

Постановление Правительства РФ от 21.03.2012 г. №211 (с изм.). Обезличивание персональных данных при их обработке в ГИС. Аттестация ГИС.

Практические работы.

Подготовка объекта к аттестации. Типовые формы документов.

Изучение методов обезличивания персональных данных.

III. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по дополнительной общеразвивающей программе: 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 литератур, Интернет-ресурсов
«Организация обработки и защиты персональных данных»	– печатные раздаточные материалы для слушателей – электронные ресурсы 1. Электронная база данных «Scopus» (http://www.scopus.com); 2. Электронная библиотечная система Алтайского государственного университета (http://elibrary.asu.ru/); 3. Научная электронная библиотека elibrary (http://elibrary.ru) www.gpntb.ru/ Государственная публичная научно-техническая библиотека. www.nlr.ru/ Российская национальная библиотека. www.nns.ru/ Национальная электронная библиотека. www.rsl.ru/ Российская государственная библиотека. www.microinform.ru/ Учебный центр компьютерных технологий «Микроинформ». www.tests.specialist.ru/ Центр компьютерного обучения МГТУ им. Н.Э.Баумана. www.intuit.ru/ Образовательный сайт. www.window.edu.ru/ Библиотека учебной и методической литературы. www.osp.ru/ Журнал «Открытые системы». www.ihtika.lib.ru/ Библиотека учебной и методической литературы.

3.3. Материально-технические условия реализации программы

Наименование аудиторий	Вид занятий	Наименование оборудования, программного обеспечения
Мастерская «Корпоративная защита от внутренних угроз информационной безопасности»	все занятия	Компьютеры и программное обеспечение по количеству слушателей мультимедийный проектор, экран, доска, флипчарт Оборудование, оснащение рабочих мест, инструменты и расходные материалы – в соответствии с инфраструктурным листом по компетенции Ворлдскиллс

IV. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

4.1. Контрольно – измерительный материал по дополнительной общеразвивающей программе «Организация обработки и защиты персональных данных»

1. Карта компетенций, формируемых дополнительной общеразвивающей программой

Компетенции/контролируемые этапы	Показатели	Наименование оценочного средства
Начальный этап формирования компетенции (ий) осуществляется в период освоения программы и характеризуется освоением учебного материала		
ПК: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знать:** основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных; основные виды угроз безопасности персональных данных в информационных системах персональных данных; содержание и порядок организации работ по выявлению угроз безопасности персональных данных; процедуры задания и реализации требований по защите информации в информационных системах персональных данных; меры обеспечения безопасности персональных данных; требования по обеспечению безопасности персональных данных; порядок применения организационных мер и технических средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. **Уметь:** создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных; планировать мероприятия по обеспечению безопасности персональных данных; обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных; проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных; определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных.	**Практические работы**

	Владеть: навыками работы с правовыми базами данных; навыками определения уровней защищённости персональных данных; навыками выявления угроз безопасности персональных данных в информационных системах персональных данных; навыками разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных; навыками применения сертифицированных средств защиты информации.	
ПК: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**Знать:** критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов **Уметь:** применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих отечественных и зарубежных источниках **Владеть:** методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов навыками анализа и интерпретации информации, содержащейся в различных отечественных и зарубежных источниках	**Практические работы**
Базовый этап формирования компетенции (формируется по окончании изучения ДОП)		
ПК: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знает:** основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных; основные виды угроз безопасности персональных данных в информационных системах персональных данных; содержание и порядок организации работ по выявлению угроз безопасности персональных данных; процедуры задания и реализации требований по защите информации в информационных системах персональных данных; меры	**Вопросы по занятиям**

	обеспечения безопасности персональных данных; требования по обеспечению безопасности персональных данных; порядок применения организационных мер и технических средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. **Умеет:** создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных; планировать мероприятия по обеспечению безопасности персональных данных; обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных; проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных; определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных. **Владеет:** навыками работы с правовыми базами данных; навыками определения уровней защищённости персональных данных; навыками выявления угроз безопасности персональных данных в информационных системах персональных данных; навыками разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных; навыками применения сертифицированных средств защиты информации.	
ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**Знать:** критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов **Уметь:** применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; собирать, анализировать и	**Вопросы по занятиям**

	интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих отечественных и зарубежных источниках **Владеть:** методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов навыками анализа и интерпретации информации, содержащейся в различных отечественных и зарубежных источниках	

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Сопоставление шкал оценивания

4-балльная шкала (уровень освоения)	Отлично (повышенный уровень)	Хорошо (базовый уровень)	Удовлетворительно (пороговый уровень)	Неудовлетворительно (уровень не сформирован)
100-балльная шкала	85-100	70-84	50-69	0-49
Бинарная шкала	Зачтено			Не зачтено

Оценивание выполнения практических заданий

4-балльная шкала (уровень освоения)	Показатели	Критерии
Отлично (повышенный уровень)	1. Полнота выполнения практического задания; 2. Своевременность выполнения задания; 3. Последовательность и рациональность выполнения задания; 4. Самостоятельность решения; 5. и т.д.	Слушателем задание решено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе формул и решении нет ошибок, получен верный ответ, задание решено рациональным способом.
Хорошо (базовый уровень)		Слушателем задание решено с подсказкой преподавателя. При этом составлен правильный алгоритм решения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задание решено нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ.
Удовлетворительно (пороговый уровень)		Слушателем задание решено с подсказками преподавателя. При этом задание понято правильно, в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в выборе формул или в математических расчетах; задание решено не

		полностью или в общем виде.
Неудовлетвори-тельно (уровень не сформирован)		Слушателем задание не решено.

3. Типовые контрольные задания или иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Преподаватель самостоятельно определяет перечень типовых контрольных заданий, включает типовые контрольные задания в фонд оценочных средств.

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Перечень заданий /вопросов
1. Работа в программе Консультант Плюс. 2. Разработка модели угроз и модели нарушителя организации. 3. Подготовка объекта к аттестации. Типовые формы документов. Изучение методов обезличивания персональных данных.

ЗАДАНИЯ НА ТЕКУЩИХ ЗАНЯТИЯХ

Перечень заданий /вопросов
1. Информация, относящаяся к государственной тайне 2. Персональные данные 3. Информация, составляющая коммерческую тайну 4. Объекты информационной безопасности 5. Информационные системы и их классификация 6. Информационные процессы 7. Случайные и целенаправленные угрозы нарушения сохранности информации 8. Дезинформация 9. Риски ИБ 10. Информационное оружие 11. Информационные войны 12. Технические средства промышленного шпионажа 13. Критерии безопасности 14. “Оранжевая книга” США 15. Классы безопасности 16. Аудит информационной безопасности 17. История хакерства 18. Хакерство в России 19. Правовые механизмы защиты информации на разных уровнях 20. Понятие тайны, секрета и конфиденциальности 21. Задачи и способ функционирования межсетевого экрана 22. Политика безопасности администратора сети и брандмауэра 23. Цели интеграции межсетевых экранов