Муниципальное бюджетное образовательное учреждение
дополнительного профессионального образования
«Курсы гражданской обороны городского округа Тольятти»

Согласовано	Согласовано	Утверждаю
Глава	Руководитель департамента	Директор МБОУ ДПО
городского округа Тольятти	общественной безопасности	«Курсы ГО г.о. Тольятти»
	администрации г.о. Тольятти	
_____ Н.А. Ренц	_____ В.В. Денисов	_____ В.А. Черняков
«____» _____ 2021 г.	«14» _____ 2021 г.	«14» _____ 2021 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации
«Обеспечение безопасности персональных данных в организации»

г. Тольятти, 2021

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Программа дополнительного профессионального образования повышения квалификации «Обеспечение безопасности персональных данных в организации» (далее – Программа) разработана с учётом требований Федерального закона от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Федерального закона от 28.12.2010 г. № 390-ФЗ «О безопасности», Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятых в соответствии с ними нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», Приказа Министерства образования и науки Российской Федерации от 1.07.2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», а также документов, регламентирующих вопросы обеспечения безопасности персональных данных: «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18.02.2013 г. № 21.

Программа регламентирует обучение должностных лиц, ответственных за защиту и обработку персональных данных в организации.

Программа, исходя из местных условий, особенностей и степени подготовленности обучаемых, а также других факторов определяет расчет времени, отводимого на изучение тем, уточняет содержание тем занятий, последовательность их изучения, формы и методы проведения занятий без сокращения общего количества часов, предусмотренного настоящей Программой.

Программа подлежит ежегодной корректировке при изменениях в руководящих документах в области зашиты персональных данных.

Учебные группы для повышения квалификации комплектуются на основании поданных заявок или письменных обращений. Количество слушателей в группе не должно превышать 25 человек. Для проведения практических занятий разрешается учебную группу делить на подгруппы численностью 12-13 человек.

Продолжительность ежедневных учебных занятий с преподавателем не менее 6 учебных часов (по 45 минут). Кроме того, ежедневно (кроме предвыходных и предпраздничных дней) предусматривается 3 часа на самостоятельную работу слушателей. Часы самоподготовки используются для изучения, рекомендуемого дополнительного материала, работы с нормативными правовыми документами, консультаций, а также просмотра учебных видеоматериалов.

1.1. Цель реализации программы.

Целью реализации Программы является формирование знаний и навыков у слушателей в сфере организации работы с персональными данными, необходимых для осуществления своей деятельности в рамках выполнения требований законодательства о персональных данных.

1.2. Планируемые результаты обучения.

В результате прохождения курса повышения квалификации должностные лица, ответственные за защиту и обработку персональных данных в организации должны:

знать:

- основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;
- основные виды угроз безопасности персональных данных в информационных системах;
- содержание и порядок организации работ по выявлению угроз безопасности персональных данных;
- реализация требований по защите информации в информационных системах персональных данных;
- порядок применения организационных мер и технических средств обеспечения безопасности персональных данных при их обработке в информационных системах.
- по определению категории, обрабатываемых в информационной системе персональных данных, определению класса типовой информационной системы персональных данных;

уметь:

- 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;
- ориентироваться в действующем законодательстве, регулирующем вопросы персональных данных;
- выделять персональные данные из иных категорий конфиденциальной информации, обрабатываемых в организации;
- составлять уведомления об обработке персональных данных;
- определять категории обрабатываемых персональных данных;
- определять класс информационной системы персональных данных;
- оценивать актуальность угроз безопасности;
- подготавливать нормативно-распорядительные документы организации в целях выполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» о необходимости принятия организационных мер защиты персональных данных от неправомерных действий;

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.

1.3. Категория слушателей.

Программа предназначена для повышения квалификации:

- руководителей и сотрудников государственных, муниципальных органов, органов местного самоуправления, организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

Данная программа является программой повышения квалификации как дополнительное образование к среднему профессиональному и высшему профессиональному образованию.

1.4. Трудоемкость обучения.
- 18 часов.

1.5. Форма обучения
- очная с отрывом от работы;
- очно-заочная с применением электронных дистанционных образовательных технологий;
- заочная (дистанционная).

1.6. Режим занятий
Учебный год: круглогодичное обучение.
Сменность занятий (при очной форме обучения): 1 смена.
Количество учебных дней в неделю: 5 дней.
Продолжительность занятия: 45 минут (1 академический час).
Режим занятий для обучающихся по очной форме:

№ п/п	Проводимые мероприятия	Время проведения	
		понедельник - четверг	пятница
1.	Регистрация	8.00-8.05	8.00-8.05
2.	1-й час занятий	8.05-8.50	8.05-8.50
3.	2-й час занятий	8.55-9.40	8.55-9.40
4.	3-й час занятий	9.45-10.30	9.45-10.30
5.	4-й час занятий	10.35-11.20	10.35-11.20
6.	5-й час занятий	11.25-12.10	11.25-12.10
7.	**Обеденный перерыв**	**12.10-12.45**	**12.10-12.45**
8.	6-й час занятий	12.45-13.30	12.45-13.30
9.	7-й час занятий	13.35-14.20	13.35-14.20
10.	8-й час занятий	14.25-15.10	
11.	**Самостоятельная работа слушателей**		

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

№ п/п	Наименование разделов (модулей)	Формы обучения, виды занятий, количество часов и форма контроля														
		ОЧНАЯ						ОЧНО-ЗАОЧНАЯ						ЗАОЧНАЯ		
		Общая трудоемкость	в том числе				Форма контроля	Общая трудоемкость	в том числе				Форма контроля	Общая трудоемкость	Самостоятельно	Форма контроля
			Лекции	Семинары	Практические	Самостоятельно			Лекции	Семинары	Практические	Самостоятельно				
1.	**Раздел 1.** Введение. Общие понятия о персональных данных	**3**	3				СК	**3**	2			1	СК	**3**	3	МК
2.	**Раздел 2.** Основные требования руководящих документов по защите персональных данных	**3**	1				СК	**3**	2			1	СК	**3**	3	МК
3.	**Раздел 3.** Организационные меры по защите и приведению информационной системы персональных данных в соответствие с требованиями законодательства РФ	**5**	2		3		СК	**5**	1		2	2	СК	**5**	5	МК
4.	**Раздел 4.** Техническая защита персональных данных в информационных системах	**3**	3				СК	**3**	1			2	СК	**3**	3	МК
5.	**Раздел 5.** Контроль и надзор за соблюдением законодательства о персональных данных	**2**	2				СК	**2**	1			1	СК	**2**	2	МК
	Итоговая аттестация	**2**						**2**						**2**		
	ИТОГО	**18**	**13**		**3**			**18**	**7**		**2**	**7**		**18**	18	

Примечание: УК – устный контроль; МК – машинный (программированный) контроль;
ТК – тестовый контроль; СК – самоконтроль.

2.2. Учебно-тематический план

№ темы занятий	Наименование разделов и тем занятий	Формы обучения, виды занятий, количество часов и форма контроля														
		ОЧНАЯ						ОЧНО-ЗАОЧНАЯ						ЗАОЧНАЯ		
		Всего	в том числе				Форма контроля	Всего	в том числе				Форма контроля	Всего	Самостоятельно	Форма контроля
			Лекции	Семинары	Практические	Самостоятельно			Лекции	Семинары	Практические	Самостоятельно				
Раздел 1. Введение. Общие понятия о персональных данных																
1.	Законодательство Российской Федерации об обработке и защите персональных данных	1	1				СК	1	0,5			0,5	СК	1	1	МК
2.	Понятие персональных данных. Специальные категории персональных данных. Биометрические персональные данные	1	1				СК	1	0,5			0,5	СК	1	1	МК
3.	Права субъекта персональных данных. Обязанности оператора персональных данных	1	1				СК	1	0,5			0,5	СК	1	1	МК
Раздел 2. Основные требования руководящих документов по защите персональных данных																
1.	Перечень основных руководящих документов по защите персональных данных	1	1				СК	1	0,5			0,5	СК	1	1	МК
2.	Основные требования документов	1	1				СК	1	0,5			0,5	СК	1	1	МК
3.	Ответственность за нарушение требований законодательства РФ «О персональных данных»	1	1				СК	1				1	СК	1	1	МК
Раздел 3. Организационные меры по защите и приведению информационной системы персональных данных в соответствие с требованиями законодательства РФ																
1.	Алгоритм работы оператора для выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»	2	1		1		УК	2	0,5		0,5	1	УК	2	2	МК
2.	Внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие	2	1		1		УК	2	0,5		0,5	1	УК	2	2	МК
3.	Подготовка уведомлений об обработке персональных данных в уполномоченный орган	1			1		УК	1			1		УК	1	1	МК
Раздел 4. Техническая защита персональных данных в информационных системах																
1.	Классификация информационных систем персональных данных	1	1				СК	1	0,5			0,5	СК	1	1	МК
2.	Методика разработки частной модели угроз для организации и определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных	1	1				СК	1	0,5			0,5	СК	1	1	МК
3.	Технические методы защиты персональных данных. Образцы продуктов защиты информации	1	1				СК	1	0,5			0,5	СК	1	1	МК

№ темы занятий	Наименование разделов и тем занятий	Формы обучения, виды занятий, количество часов и форма контроля														
		ОЧНАЯ						ОЧНО-ЗАОЧНАЯ						ЗАОЧНАЯ		
		Всего	в том числе			Самостоятельно	Форма контроля	Всего	в том числе			Самостоятельно	Форма контроля	Всего	Самостоятельно	Форма контроля
			Лекции	Семинары	Практические				Лекции	Семинары	Практические					
Раздел 5. Контроль и надзор за соблюдением законодательства о персональных данных																
1.	Регламент проведения проверок. Плановые и внеплановые проверки	1	1				СК	1	0,5			0,5	СК	1	1	МК
2.	Форма проведения проверки. Оформление результатов проверки	1	1				СК	1	0,5			0,5	СК	1	1	МК
	Итоговый контроль (зачет)	**2**			**2**		**ТК**	**2**			**1**	**1**	**ТК**	**2**	**2**	**МК**
	ИТОГО	**18**	**13**		**5**			**18**	**6**		**3**	**9**		**18**	**18**	

<u>Примечание:</u> УК – устный контроль; МК – машинный (программированный) контроль;
ТК – тестовый контроль; СК – самоконтроль.

2.3. Календарный учебный график по освоению программы дополнительного профессионального образования повышения квалификации «Обеспечение безопасности персональных данных в организации» в МБОУ ДПО «Курсы ГО г.о. Тольятти»

Наименование мероприятий	Дни недели				
	Понедельник	Вторник	Среда	Четверг	Пятница
Раздел 1. Введение. Общие понятия о персональных данных	3 час.				
Раздел 2. Основные требования руководящих документов по защите персональных данных	3 час.				
Раздел 3. Организационные меры по защите и приведению информационной системы персональных данных в соответствие с требованиями законодательства РФ		5 час.			
Раздел 4. Техническая защита персональных данных в информационных системах		1 час.	2 час.		
Раздел 5. Контроль и надзор за соблюдением законодательства о персональных данных			2 час.		
Самостоятельная работа					
Итоговая аттестация (зачет)			2 час.		

Итого: 18 часов

Примечание: учреждение вправе самостоятельно выстраивать структурно-логическую схему (последовательность) изучения модулей (тем занятий) исходя из логичности изложения учебного материала и по другим причинам.

2.4. Содержание программы дополнительного профессионального образования повышения квалификации «Обеспечение безопасности персональных данных в организации»

Раздел 1. Введение. Общие понятия о персональных данных.

Учебные вопросы:

1. Защита персональных данных как реализация конституционных прав граждан на неприкосновенность частной жизни. Персональные данные в системе документооборота предприятия. Персональные данные в автоматизированных системах и приложениях. Значимые утечки персональных данных в России и примеры неправомерного использования персональных данных.

2. Понятия: «персональные данные», «оператор персональных данных», «обработка персональных данных», «информационная система персональных данных», «регуляторы». Категории персональных данных. Две категоризации персональных данных. Категории персональных данных по Федеральному закону «О персональных данных»: общедоступные, специальные, биометрические. Категории персональных данных по совместному приказу ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»: 1 категория, 2 категория, 3 категория, 4 категория.

3. Права субъекта персональных данных. Кто такой «субъект персональных данных». Рассмотрение основных его прав по Федеральному закону № 152 «О персональных данных». Обязанности оператора персональных данных. Рассмотрение основных обязанностей операторов по Федеральному закону №152 «О персональных данных». Контроль со стороны Роскомнадзора, ФСБ и ФСТЭК.

Раздел 2. Основные требования руководящих документов по защите персональных данных.

Учебные вопросы:

1. Нормативные акты в области персональных данных. Перечень основных регулирующих правовых и нормативных актов. Содержание и основные положения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». Указ Президента Российской Федерации от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». Федеральный Закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Постановление Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных. Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Приказ Роскомнадзора России от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных». Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных использованием средств

криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

2. Ответственность за нарушение требований законодательства по обеспечению безопасности персональных данных. Административная ответственность: нарушения и наказания. Уголовная ответственность: типовые нарушения и наказания.

Раздел 3. Организационные меры по защите и приведению информационной системы персональных данных в соответствие с требованиями законодательства Российской Федерации.

Учебные вопросы:

1. Мероприятия по защите сведений ограниченного доступа. Практические шаги по приведению порядка обработки в соответствие с требованиями законодательства. Ограничение доступа к персональным данным. Учет лиц, допущенных к персональным данным. Определение порядка обращения с такими сведениями, контроля за его соблюдением.

2. Локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, их содержание, порядок разработки и ввода в действие. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Защита персональных данных в кадровой документации. Принципы защиты персональных данных работников организации. Журнал учета персональных данных и порядок его ведения. Хранение и уничтожение материальных носителей с информацией о персональных данных. Сроки хранения. Порядок уничтожения. Порядок реализации мер по обеспечению безопасности персональных данных.

3. Подготовка уведомлений об обработке персональных данных в уполномоченный орган. Порядок внесения изменений в сведения в реестре операторов, осуществляющих обработку персональных данных.

Раздел 4. Техническая защита персональных данных в информационных системах.

Учебные вопросы:

1. Особенности обеспечения безопасности персональных данных в автоматизированных системах. Классификация автоматизированных систем. Классы защищенности. Обеспечение безопасности в автоматизированных рабочих местах (АРМ) на базе автономных ПЭВМ при использовании съемных накопителей большой емкости. Обеспечение безопасности в локальных вычислительных сетях. Обеспечение безопасности при межсетевом взаимодействии. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Обезличивание персональных данных. Информационная система персональных данных. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн. Перечень необходимых мероприятий.

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Разработка организационно-распорядительных документов по технической защите персональных данных. Выбор и применение аппаратно-программных средств, используемых в системах технической защиты персональных данных при их обработке в информационных системах.

Раздел 5. Контроль и надзор за соблюдением законодательства о персональных данных.

Учебные вопросы:

1. Система государственного контроля и надзора за обеспечением безопасности персональных данных. Порядок планирования, организации и проведения проверок. Права и обязанности проверяемых и проверяющих.

2. Меры, принимаемые должностными лицами органа госконтроля (надзора) при выявлении фактов нарушений. Меры, принимаемые должностными лицами органа госконтроля (надзора) при выявлении фактов нарушений.

III. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

По окончании процесса обучения проводится итоговая аттестация в форме тестирования. Итоговая аттестация знаний слушателей производится аттестационной комиссией. Состав аттестационной комиссии утверждается приказом директора учреждения. При успешном прохождении итоговой аттестации слушателям выдается удостоверение о повышении квалификации установленного образца.

Примерные вопросы для подготовки к зачёту:

1. Права и обязанности граждан РФ в отношении своих персональных данных.
2. Правовое оформление режима коммерческой тайны и работы с персональными данными в рамках трудовых отношений.
3. Коммерческая тайна и базы персональных данных как объекты интеллектуальной собственности организации.
4. Правовое оформление режима коммерческой тайны работы с персональными данными в рамках гражданско-правовых отношений.
5. Работа с персональными данными в рамках гражданско-правовых отношений.
6. Режим защиты персональных данных в организации.
7. Обоснование системы технической защиты персональных данных в организации.
8. Базовые технологии и средства технической защиты персональных данных.
9. Применение криптографических сервисов для защиты персональных данных.
10. Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации.
11. Порядок проведения проверок территориальными подразделениями Роскомнадзора.
12. Разработка частных моделей угроз ИСПД.
13. Разработка требований безопасности к ИСПД и внедрение защитных мероприятий.
14. Оценка соответствия ИСПД требованиям безопасности.
15. Приведение эксплуатируемых информационных систем персональных данных в соответствие с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».
16. Разработка организационно-распорядительных документов по защите персональных данных в организации.
17. Основные положения Федерального Закона «О персональных данных».
18. Основные требования «Положения об обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных».
19. Структура методических документов ФСТЭК России по обеспечению безопасности персональных данных.
20. Угрозы безопасности персональным данным при их обработке в информационных системах персональных данных.
21. Модель угроз безопасности персональным данным. Методика выявления актуальных угроз безопасности персональным данным.
22. Формирование модели угроз безопасности персональным данным.
23. Организация работ по созданию системы технической защиты персональных данных при их обработке в информационных системах. Рекомендации по разработке организационно-распорядительных документов по технической защите персональных данных.
24. Выбор и применение аппаратно-программных средств, используемых в системах технической защиты персональных данных при их обработке в информационных системах.

IV. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

4.1. Учебно-методическое и информационное обеспечение

Нормативные правовые акты

1. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981 г.).
2. Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
3. Федеральный закон от 30.12.2001 г. № 197-ФЗ «Трудовой кодекс Российской Федерации».
4. Федеральный закон от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи».
5. Федеральный закон от 19.12.2005 г. №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
6. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон от 27.07 2006 г. №152-ФЗ «О персональных данных».
8. Федеральный закон от 29.12.2012 г. №273-ФЗ «Об образовании в Российской Федерации».
9. Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи».
10. Федеральный закон от 21.07.1993 г. № 5485-1 «О государственной тайне».
11. Постановление Правительства РФ от 15.09.2008 г. №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
12. Постановление Правительства РФ от 6.07.2008 г. №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
13. Постановление Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
14. Постановление Правительства РФ от 21.03.2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
15. Постановление Правительства РФ от 06.09.2014 г. №911 «О внесении изменений в перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
16. Постановление Правительства России от 10.07.2013 г. №582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации».
17. Постановление Правительства России от 16.03.2009 г. №228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»).
18. Распоряжение Правительства РФ от 29.12.2014 г. № 2769-р «Об утверждении

Концепции региональной информатизации» (раздел «Программно-аппаратные средства обеспечения информационной безопасности»).

19. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 15.02.2008 г.

20. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14.02.2008 г.

21. Приказ ФСТЭК России от 5.02.2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».

22. Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

23. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

24. «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», утверждены заместителем директора ФСТЭК России 15.02.2008 г.

25. Приказ ФСБ РФ от 09.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

26. Приказ ФСБ РФ от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

27. Приказ ФСБ РФ от 31.03.2015 г. № 149/7/2/6-432 «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности».

28. Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

29. Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ»).

Учебная литература

1. Аверченков, В. И. Защита персональных данных в организации / В.И. Аверченков. - М.: Флинта, 2016. - 124 с.

2. Бойкова, О.Ф. Защита персональных данных: касается всех! Практическое пособие. Выпуск № 142 / О.Ф. Бойкова. - М.: Либерея, 2012. - 95 с.

3. Емельянова, Н. З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2009. - 368 с.

4. Кин, Эндрю Ничего личного. Как социальные сети, поисковые системы и спецслужбы используют наши персональные данные для собственной выгоды / Эндрю Кин. - М.: Альпина Паблишер, 2016. - 224 с.

5. Лушников А. М. Защита персональных данных работника: сравнительно-правовой комментарий гл.14 Трудового Кодекса РФ. [Электронный ресурс]. — Режим доступа: https://www.top-personal.ru/issue.html?2150 (дата обращения: 24.08.2020).

6. Макаров А. М. Организация защиты персональных данных: учебное пособие / А. М. Макаров, И. В. Калиберда, К. О. Бондаренко. — Ставрополь: СКФУ, 2015. - 102 с.

7. Сабанов, А. Г. Защита персональных данных в организациях здравоохранения: учебное пособие / А. Г. Сабанов, В. Д. Зыков, Р. В. Мещеряков. — Москва: Горячая линия-Телеком, 2012. - 206 с.

8. Савельев, А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» / Савельев Александр Иванович. - М.: Статут, 2017. - 470 с.

9. Филиппов, П. Б. Использование и защита персональных данных в социальных сетях Интернета / П.Б. Филиппов. - М.: Синергия, 2012. - 133 с.

Перечень информационных ресурсов в сети Интернет

1. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) (https://rkn.gov.ru/).

2. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) (https://digital.gov.ru/ru/).

3. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) (https://fstec.ru/).

4. Журнал «Информационная безопасность» (https://www.itsec.ru/).

5. Профессиональные базы данных:

- Электронная база данных «Scopus» (http://www.scopus.com).
- Научная электронная библиотека elibrary (http://elibrary.ru).
- Государственная публичная научно-техническая библиотека (www.gpntb.ru/).
- Российская национальная библиотека (www.nlr.ru/).
- Национальная электронная библиотека (www.nns.ru/).
- Российская государственная библиотека (www.rsl.ru/).
- Библиотека учебной и методической литературы (www.window.edu.ru/).
- Библиотека учебной и методической литературы (www.ihtika.lib.ru/).

4.2. Материально-техническое обеспечение

Обучение проводится на учебно-методической базе Учреждения.

В процессе обучения применяются современные технические средства обучения и методические пособия, разработанные по темам Программы.

Оборудование учебного кабинета:

- рабочие места по количеству обучающихся (стол, стул, необходимые для работы в аудитории канцелярские принадлежности);
- рабочее место преподавателя (стол, стул, необходимые для работы в аудитории канцелярские принадлежности);
- доска для записей с принадлежностями (маркеры для письма, указка).

Технические средства обучения:

- персональный компьютер преподавателя с периферийными устройствами и доступом к сети Интернет;
- мультимедиа-проектор с экраном.

Слушателям выдаются учебно-методические материалы (презентации преподавателей, конспекты, нормативные правовые акты, образцы рассматриваемых на

занятиях документов, примеры решения практических задач, статьи и другие материалы по темам Программы) в электронном виде и отдельные материалы на бумажном носителе, которые являются неотъемлемой частью процесса обучения.

4.3. Кадровые условия

К преподаванию учебной Программы привлекаются преподаватели, имеющие большой опыт педагогической деятельности (более 5 лет).

Рабочая учебная программа дополнительного профессионального образования, повышения квалификации «Обеспечение безопасности персональных данных в организации» разработана авторским коллективом МБОУ ДПО «Курсы гражданской обороны г.о. Тольятти».

Программа обсуждена и одобрена на заседании педагогического совета МБОУ ДПО «Курсы гражданской обороны городского округа Тольятти». Протокол №26 от 30 августа 2021 года.