ГАУ Калининградской области
«Калининградский государственный научно-исследовательский центр информационной и технической безопасности» (КГ НИЦ)

«Утверждаю
И.о. директора КГ НИЦ
_____ Сергеева Ю.Г.
«___» _____2022 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

повышения квалификации

«ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ»

(72 часа)

Калининград, 2022

1. Цель программы

Целью обучения по дополнительной профессиональной программе (ДПП) является развитие компетенций в текущей деятельности руководителей и специалистов государственных и муниципальных органов управления, учреждений, организаций всех форм собственности, включая индивидуальных предпринимателей и самозанятых, в части соответствия квалификационным требованиям и развития профессиональных качеств, необходимых для планирования, организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации.

Поставленная цель достигается решением следующих задач:

- изучением актуальных нормативных правовых и организационных основ обеспечения безопасности персональных данных в информационных системах;
- изучением современных методов и процедур выявления угроз безопасности персональных данных в информационных системах и оценки степени их опасности;
- практической отработкой способов и порядка проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах.

2. Планируемые результаты освоения программы

Повышение квалификации сотрудников, ответственных за защиту информации в органах исполнительной власти и подведомственным им государственным учреждениям, а также сотрудников предприятий, учреждений и организаций любой формы собственности, включая индивидуальных предпринимателей и самозанятых, по программе «Обеспечение безопасности персональных данных при их обработке в информационных системах» направлено на совершенствование и актуализацию необходимых в их деятельности профессиональных и профессионально-специализированных компетенций. В результате изучения курса обучающие должны

1) знать:

– содержание основных актуальных 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;

2) уметь:

– планировать мероприятия по обеспечению безопасности персональных данных;

– разрабатывать необходимые документы в интересах организации работ по обеспечению безопасности персональных данных;

– проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах;

– определять состав и содержание мер по обеспечению безопасности персо-

нальных данных при их обработке в информационных системах, необходимых для блокирования угроз безопасности персональных данных.

3) иметь навык:

– определения уровня защиты персональных данных;

– выявления угроз безопасности персональных данных в информационных системах;

– работы с нормативными правовыми актами в области защиты информации и обеспечения безопасности информации в ключевых системах информационной инфраструктуры.

3. Категория слушателей:

3.1 Образование: высшее, среднее профессиональное.

3.2 Квалификация: руководители и специалисты государственных и муниципальных органов исполнительной власти, учреждений, организаций всех форм собственности, включая индивидуальных предпринимателей и самозанятых, трудовые функции которые связаны с получением, использованием, хранением, формированием баз персональных данных.

3.3 Наличие опыта профессиональной деятельности: желательно.

3.4 Предварительное освоение иных дисциплин/ курсов/ модулей: умение использовать информационно-компьютерные технологии при работе с персональными данными.

4. Учебный план дополнительной профессиональной программы (повышения квалификации) **«Обеспечение безопасности персональных данных при их обработке в информационных системах»**

№ п/п	Наименование учебных модулей	Всего часов	Виды учебных занятий		
			лекции, ч	практические занятия, ч	самостоятельная работа, ч
1	Модуль 1 Общие вопросы технической защиты информации	24	8	6	10
2	Модуль 2 Организации обеспечения безопасности персональных данных в информационных системах	46	14	10	22
3	Итоговая аттестация	2		2	
4	Всего:	72	22	18	32

5. Учебно-тематический план программы «Обеспечение безопасности персональных данных при их обработке в информационных системах»

№ п/п	Наименование учебных модулей	Всего часов	Виды учебных занятий			Формы контроля
			лекции, ч	практические занятия, ч	самостоятельная работа, ч	
1	Модуль 1 Общие вопросы технической защиты информации	24	8	6	10	
1.1	Тема 1.1 Правовые и организационные основы технической защиты информации ограниченного доступа	10	4		6	
1.2	Тема 1.2 Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	14	4	6	4	реферат
2	Модуль 2 Организации обеспечения безопасности персональных данных в информационных системах персональных данных	46	14	10	22	
2.1	Тема 2.1 Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах	20	6	6	8	
2.2	Тема 2.2 Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах	20	6		14	
2.3	Тема 2.3 Практические реализации типовых моделей защищённых информационных систем обработки персональных данных	6	2	4		
3	Итоговая аттестация	2		2		зачет
4	Всего:	72	22	18	32	

6. Учебная (рабочая) программа повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах»

Модуль 1 Общие вопросы технической защиты информации (24 ч)

Тема 1.1 Правовые и организационные основы технической защиты информации ограниченного доступа (10 ч)

Основные понятия в области технической защиты информации (ТЗИ). Стратегия национальной безопасности Российской Федерации до 2020 года. Доктрина информационной безопасности Российской Федерации. Концептуальные основы ТЗИ. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих. Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации, их задачи, распределение полномочий по обеспечению ТЗИ. Задачи, полномочия и права Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Задачи, полномочия и права управлений ФСТЭК России по федеральным округам.

Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Документы национальной системы стандартизации в области ТЗИ.

Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.

Тема 1.2 Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа (14 ч)

Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность и доступность информации. Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы оценки опасности угроз.

Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак, реализуемых в информационно-телекоммуникационных сетях.

Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования.

Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.

Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.

Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

Модуль 2 Организация обеспечения безопасности персональных данных в информационных системах (46 ч)

Тема 2.1 Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных (20 ч)

Особенности информационного элемента информационной системы. Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах, порядок их определения. Угрозы несанкционированного доступа к информации в информационных системах персональных данных. Угрозы утечки информации по техническим каналам.

Основные принципы обеспечения безопасности персональных данных при их обработке: законности, превентивности, адекватности, непрерывности, адаптивности, самозащиты, многоуровневости, персональной ответственности и минимизации привилегий, разделения полномочий и их характеристика. Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах. Общий порядок организации обеспечения безопасности персональных данных в информационных системах. Оценка достаточности и обоснованности запланированных мероприятий.

Особенности обеспечения безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах с использованием автономных ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии. Рекомендации по применению мер и средств обеспечения безопасности персональных данных от физического доступа.

Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации. Классификация ТКУИ.

Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях.

Оценка защищённости информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации.

Тема 2.2 Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах (20 ч)

Определение необходимых уровней защищенности персональных данных при их обработке в информационных системах в зависимости от типа актуальных угроз для информационных систем, вида и объема обрабатываемых в них персональных данных.

Состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий.

Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных: определение базового набора Мер, адаптация базового набора, уточнение адаптированного базового набора мер, дополнение уточненного адаптированного базового набора мер.

Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных. Требования к средствам защиты информации для обеспечения различных уровней защищенности персональных данных. Организация обеспечения безопасности персональных данных в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных. Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и особенности их реализации.

Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Подготовка уведомлений об обработке персональных данных в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление.

Обязанности оператора, осуществляющего обработку персональных данных. Порядок и условия обработки персональных данных без средств автоматизации. Порядок и методы обезличивания персональных данных, их деобезличивание. Особенности обработки персональных данных в условиях государственной гражданской службы и муниципальной службы. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.

Тема 2.3 Практические реализации типовых моделей защищенных информационных систем обработки персональных данных (6 ч)

Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, разверты-

ваемой в информационной системе персональных данных в процессе ее создания или модернизации. Основное содержание этапов организации обеспечения безопасности персональных данных.

Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации.

Виды, формы и способы контроля защиты персональных данных в информационных системах. Планирование работ по контролю состояния защиты персональных данных в информационных системах. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты персональных данных.

Перечень практик-ориентированных заданий

№ п/п	Номер темы	Наименование практического занятия	Описание
1	Тема 1.2	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	*Ситуационная задача.* Определение перечня организационных и технических мер, необходимых для нейтрализации угроз учреждения (организации)
2	Тема 2.1	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах	*Ситуационная задача.* Определение перечня организационных и технических мер, по выполнению требований законодательства РФ при обработке персональных данных.
3	Тема 2.3	Практические реализации типовых моделей защищённых информационных систем обработки персональных данных.	*Ситуационная задача.* Составление плана внутренних проверок по защите информации учреждения (организации).

Выполнение практик-ориентированных заданий позволяет решить конкретные проблемы обеспечения защиты персональных данных в организациях, учреждениях в соответствии с требованиями регуляторов.

7. Оценочные материалы по образовательной программе

7.1 Вопросы тестирования по модулям

№ п/п	Вопросы промежуточного контроля (тематика рефератов)	Вопросы итогового тестирования
1	Организация работ по обработке ПДн.	Раскройте правовое и нормативное обеспечение защиты ПДн.
2	Права субъекта ПДн.	Что относится к персональным данным в соответствии с требованиями нормативно-правовой базы РФ?
3	Модель угроз безопасности ПДн.	Охарактеризуйте порядок хранения и использования ПДн в организациях РФ.

4	Угрозы информации в ИСПДн.	На что направлена деятельность по защите ПДн?На основе каких принципов осуществляется защита ПДн?
5	Классификация ИСПДн.	Перечислите категории и виды ПДн.
6	Идентификация и аутентификация пользователей.	Назовите возможные пути утраты ПДн.
7	Организационные меры защиты информации в информационных системах.	Перечислите основные обязанности и права работников с целью обеспечения защиты персональных данных, хранящихся у работодателя.
8	Методы обнаружения известных и неизвестных вирусов.	Назовите особенности обработки ПДн в государственных ИСПДн.
9	Функции администратора по созданию и управлению учетными записями пользователей.	Назовите нормативно-правовые документы РФ, являющиеся базой для создания системы защиты ПДн.
10	Нормативная база обработки ПДн.	Назовите основные положения Федерального закона Российской Федерации от 27 июля 2006 года ФЗ-№152 «О персональных данных».
11	Принципы обработки ПДн.	Какова ответственность за нарушение правил работы с ПДн работников.
12	Биометрические ПДн.	Особенности обработки ПДн, осуществляемой без использования средств автоматизации.
13	Права субъекта ПДн.	Особенности обработки ПДн, обрабатываемых в ИСПДн.
14	Обязанности оператора.	Базовая модель угроз безопасности ПДн при их обработке в ИСПДн.
15	Меры по обеспечению безопасности ПДн при их обработке.	Классификация угроз безопасности ПДн, обрабатываемых в ИСПДн.
16	Ответственность за нарушения в области обработки ПДн.	Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн.
17	Защита ПДн от несанкционированного доступа.	Охарактеризуйте этапы построения модели угроз безопасности ПДн, обрабатываемых в ИСПДн.
18	Обработка персональных данных, осуществляемая без использования средств автоматизации.	Назовите основные мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн.
19	Разработка модели угроз безопасности ПДн с учетом методических документов регуляторов.	Назначение и способы обеспечения доступности ПДн.
20	Требования к защите информации, содержащейся в информационной системе.	Назначение выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности

		ПДн, и реагирование на них.
21	Разработка системы защиты информации информационной системы.	Условия обработки ПДн.
22	Аттестация информационной системы.	Назначение средств обнаружения (предотвращения) вторжений.
23	Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы.	Модель угроз ИСПДн. Методика разработки.
24	Содержание мер по обеспечению безопасности ПДн.	Контроль и надзор за выполнением требований по обеспечению безопасности ПДн.
25	Требования и методы по обезличиванию ПДн.	Назначение и способы защиты машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн.
26		Особенности гарантированного уничтожения информации на магнитных носителях с использованием магнитных воздействий.
27		Особенности гарантированного уничтожения информации на оптических носителях с использованием редуцирующего механического воздействия.
28		Особенности гарантированного уничтожения информации на полупроводниковых носителях с использованием термических воздействий.
29		Перечислить и описать угрозы безопасной передачи данных в телекоммуникационных системах.
30		Перечислить и описать задачи защиты информации в телекоммуникационных системах.
31		Перечислить и описать механизмы защиты информации в телекоммуникационных системах.

7.2 Описание показателей и критериев оценивания, шкалы оценивания

Уровень освоения	Критерии освоения	Показатели и критерии оценки сформированности компетенции	Шкала оценивания
Продвинутый	*Компетенция сформирована.* Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка	Теоретическое содержание программы освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения задания выполнены, качество их выполнения оценено на максимальную оценку. Обучающийся демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или	**Зачтено** более 90% правильных ответов

		нестандартных заданий в рамках трудовой функции с использованием ***знаний, умений и навыков,*** полученных в ходе освоения данной программы.	
Базовый	*Компетенция сформирована.* Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка	Теоретическое содержание программы освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, но некоторые виды заданий выполнены с несущественными ошибками. Способность обучающегося продемонстрировать самостоятельное применение ***знаний, умений и навыков*** при решении стандартных заданий.	**Зачтено** более 75% правильных ответов
Пороговый	*Компетенция сформирована.* Демонстрируется недостаточный уровень самостоятельности практического навыка	Теоретическое содержание программы освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки. Если обучаемый демонстрирует самостоятельность в применении ***знаний, умений и навыков*** к решению стандартных заданий в рамках трудовых функций, то следует считать, что компетенция сформирована, но ее уровень недостаточно высок.	**Зачтено** более 60% правильных ответов
Низкий	*Компетенция не сформирована* Демонстрируется отсутствие *или* фрагментарное наличие самостоятельности и практического навыка	Теоретическое содержание программы не освоено, необходимые практические навыки работы с освоенным материалом не сформированы, выполненные учебные задания содержат ошибки. Неспособность обучаемого самостоятельно продемонстрировать наличие ***знаний*** при реализации трудовой функции, отсутствие самостоятельности в применении ***умения*** и неспособность самостоятельно проявить ***навык*** повторения решения стандартных задач по обеспечению защиты персональных данных свидетельствуют об отсутствии сформированной компетенции.	**не зачтено** менее 60% правильных ответов

7.3. Примеры контрольных заданий по модулям/ программы

Кейс «Кадровый учет в компании»

Численный состав работников ООО «Х» насчитывает около 50 чел. Поскольку штат небольшой, персональные данные работников обрабатываются исключительно на бумажных носителях информации и не заносятся ни в какую информационную систему.

При этом отличительным свойством кадровой политики организации является текучесть персонала, которая не является исключением и для отдела кадров.

Задание. Исходя из текущей ситуации подготовьте перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ в

соответствии с требованиями п. 13 постановления Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Кейс «Уровень защищенности информационной системы персональных данных»

Определите уровень защищенности информационной системы персональных данных для следующих организаций:

1) банк;
2) медицинская организация;
3) торговая сеть.

Для определения категорий персональных данных, обрабатываемых в организации, воспользуйтесь реестром операторов, осуществляющих обработку (https://pd.rkn.gov.ru/operators-registry/operators-list).

По итогам работы подготовьте проект акта определения уровня защищенности.

Кейс «Внедрение Microsoft Office 365»

Руководством международной компании, имеющей представительство в Российской Федерации, было принято решение о внедрении облачного сервиса Microsoft Office 365. Технические средства сервиса Microsoft Office 365 находятся за рубежом (за пределами территории РФ), при этом компания планирует при помощи Microsoft Office 365 осуществлять обработку персональных данных работников — граждан Российской Федерации.

Задание. Предложите решение по организации обработки персональных данных работников в облачном сервисе Microsoft Office 365, соответствующее нормам действующего законодательства РФ.

7.4. Примеры контрольных заданий для проведения итоговой аттестации

1 Вопрос: Не могут относиться к коммерческой тайне (дайте несколько вариантов ответов):

1 сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;
2 сведения, разглашение которых наносит ущерб;
3 документы об уплате налогов и других обязательных платежей.

2 Вопрос: Организационные меры защиты коммерческой тайны — это (дайте несколько вариантов ответов)...

1 разработка системы защиты информации;
2 организация конфиденциального делопроизводства;
3 создание режимного подразделения.

3 Вопрос: Персональные данные — это сведения:

1 составляющие коммерческую тайну;
2 конфиденциального характера;

3 составляющие государственную тайну.

4 Вопрос: Для больших помещений с количеством окон более 5 или большой площадью непрерывного остекления количество открывающихся решеток определяется...

1 условиями освещенности;
2 условиями быстрой эвакуации людей;
3 высотности здания.

5 *Вопрос: Обеспечение сохранности и конфиденциальности предполагает (дайте несколько вариантов ответов)...*

1 полноту документной информации;
2 поддержание специальных условий хранения;
3 создание специальных условий хранения.

6 *Вопрос: Какие меры обеспечения информационной безопасности нужно учесть при составлении уведомления в РосКомНадзор?*

1 меры, предусмотренные Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
2 меры, в соответствии ПП РФ от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
3 меры, в соответствии с ПП РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных»;
4 все из перечисленных.

7 Вопрос: Каким НПА регулируется служебная тайна?

1 Федеральный закон от 29.07.2004 № 98-ФЗ;
2 Федеральный закон от 27.07.2006 № 149-ФЗ;
3 Постановление Правительства РФ от 03.11.1994 № 1233.

8 Вопрос: Запирающие устройства внутренних дверей...

1 1 класса защиты;
2 2 класса защиты;
3 3 класса защиты.

9 Вопрос: В журнале учета СКЗИ необходимо учесть:

1 дистрибутивы СКЗИ, установленные программные и программно-аппаратные СКЗИ, ключевые дистрибутивы СКЗИ, листы инструктажа, заключения о подготовке к самостоятельной работе с СКЗИ;
2 дистрибутивы СКЗИ, установленые программные и программно-аппаратные СКЗИ, инструкции пользователя и администратора, формуляры, носители ЭП, ЭП;
3 дистрибутивы СКЗИ, установленные программные и программно-аппаратные СКЗИ, ключевые дистрибутивы СКЗИ, инструкции пользователя и администратора, формуляры, машинные носители.

10 Вопрос: Стадии анализа защищенности (дайте несколько вариантов ответов)...

1 подготовительная;
2 проведение анализа;

3 взлом.

11 Вопрос: Процесс взлома — это (дайте несколько вариантов ответов)...

1 эксплуатация уязвимостей;
2 уничтожение информации;
3 сканирование.

12 Вопрос: Выбор оконных конструкций и материалов, из которых они изготовлены , их класс защиты определяется исходя (дайте несколько вариантов ответов):

1 из категории охраняемого объекта;
2 из характеристик конструкции;
3 из класса обрабатываемой информации.

13 Вопрос: Чем ГИС отличается от ИС (дайте несколько вариантов ответов)?

1 оператором ГИС является только государственный орган;
2 ГИС создается для реализации полномочий госорганов;
3 ГИС создается для осуществления информационного обмена между госорганами.

14 Вопрос: Ограничительная отметка на документе конфиденциального характера используется...

1 при конфиденциальной переписке между коммерческими организациями;
2 при конфиденциальной переписке с органами исполнительной власти;
3 при переписке с органом по аттестации требованиям безопасности.

15 Вопрос: Запирающие устройства входных и запасных дверей в здание, входных дверей охраняемых помещений, дверей , выходящих на крышу (чердак) — это...

1 1 класса защиты;
2 2 класса защиты;
3 3 класса защиты.

16 Вопрос: Цели защиты — это предотвращения (дайте несколько вариантов ответов)...

1 шпионажа;
2 кражи;
3 нарушение режима.

17 Вопрос: Организация работы с документами — это (дайте несколько вариантов ответов)…

1 создание, изготовление;
2 классификация, систематизация, подготовка для архивного хранения, уничтожение;
3 учет, размножение, прохождение, исполнение, отправление.

18 Вопрос: Инструкция по конфиденциальному делопроизводству в организации…

1 запрашивается в ФСТЭК России;
2 разрабатывается в организации;
3 разрабатывается органом по аттестации требованиям безопасности.

19 Вопрос: Какие средства защиты могут применяться в системе, подключенной к ГИС?

1 только сертифицированные средства защиты информации, имеющие действующие сертификаты ФСТЭК или Роскомнадзора;

2 только сертифицированные средства защиты информации, имеющие действующие сертификаты ФСТЭК или ФСБ;

3 лицензионные средства защиты, наличие сертификата не является обязательным требованием.

20 Вопрос: Для подключения к ГИС необходимо (дайте несколько вариантов ответов):

1 провести классификацию ИС и определить угрозы безопасности;

2 разработать систему защиты информации , информационной системы;

3 аттестовать ИСПДн.

21 Вопрос: Ответственный за обработку ПДн

1 ответственность за обработку ПДн несет пользователь, непосредственно осуществляющий обработку;

2 ответственного за обработку ПДн назначает приказом руководитель учреждения;

3 руководитель учреждения несет полную ответственность за обработку ПДн и не имеет право делегировать ответственность на кого-либо.

22 Вопрос: Какой ГОСТ регламентирует методы и средства обеспечения безопасности?

1 ГОСТ РО 0043-003-2012;

2 ГОСТ РО 0043-004-2013;

3 ГОСТ Р ИСО/МЭК 27001.

23 Вопрос: В каких случаях разрешено использование средств защиты не прошедших процедуру оценки соответствия требованиям в области информационной безопасности?

1 разрешено, если СЗИ не включено в реестр отечественного программного обеспечения;

2 запрещено использование СЗИ, не прошедших данную процедуру;

3 явное ограничение не предусмотрено;

4 ответственность за выбор средства защиты лежит на операторе, вправе выбрать любое средство.

7.5. Описание процедуры оценивания результатов обучения

1. Перед итоговой аттестацией в последний учебный день, предшествующий итоговой аттестации, проводится консультация.

2. Итоговая аттестация слушателей проводится в форме тестирования, по результатам которого выставляется оценка «зачтено» (если дано 60% и более правильных ответов) или «не зачтено».

4. 3. Оценка качества освоения рабочей программы проводится в отношении:

- соответствия результатов освоения рабочей программы заявленным целям и планируемым результатам обучения;

- соответствия организации образовательной деятельности в КГ НИЦ и реализации дополнительной профессиональной программы повышения квалификации установленным требованиям к структуре, порядку и условиям реализации образовательных программ;
- способности КГ НИЦ результативно и эффективно выполнять деятельность по предоставлению образовательных услуг.

4. Слушателям, успешно освоившим программу повышения квалификации и прошедшим итоговую аттестацию, по решению аттестационной комиссии выдаются документы:
– удостоверение о повышении квалификации;
- электронный сертификат.

8. Организационно-педагогические условия реализации программы

8.1 Кадровое обеспечение программы

	ФИО преподавателя	Место основной работы, должность, ученая степень, ученое звание (при наличии)	Ссылка на веб-страницу преподавателя	Отметка о полученном согласии на обработку персональных
1	Персичкин Андрей Андреевич	КГ НИЦ, зам. директора КГ НИЦ	https://kgnic.ru/wp-content/uploads/2020/10/Persichkin-A.A.-portfolio.pdf	Получено письменное согласие
2	Хватов Дмитрий Александрович	КГ НИЦ, руководитель отдела дополнительного образования КГ НИЦ	https://kgnic.ru/wp-content/uploads/2020/10/Hvatov-D.A.-portfolio.pdf	Получено письменное согласие

8.2 Учебно-методическое сопровождение программы

Учебно-методические материалы	
Методы, формы и технологии	Методически разработки, материалы курса, учебная литература
Изучение нормативных и правовых документов, регулирующих деятельность в области защите персональных данных, в том числе в рамках самостоятельной работы, подготовки реферата и к итоговому тестированию	***9.2.1 Нормативные документы*** 1. Федеральный закон от 28.12.2010 г. № 390-ФЗ «О безопасности» 2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» 3. Федеральный закон от 24.03.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» 4. Федеральный закон от 27.12.2002 г. №184-ФЗ «О техническом регулировании» 5. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» 6. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне» 7. Указ Президента Российской Федерации от 16.08.2004 г. № Ю85 «Вопросы Федеральной службы по техническому и экспортному контролю» 8. 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» 9. Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 06.03.1997 г. № 188 10. Постановление Правительства Российской Федерации от 21.11.2011 г. № 957 «Об организации лицензирования отдельных видов деятельности» 11. Постановление Правительства Российской Федерации от 26.06.1995 г. № 608 «О сертификации средств защиты информации» 12. Постановление Правительства Российской Федерации «О лицензировании деятельности по технической защите конфиденциальной информации» от 03.02.2012 г. № 79 13. Постановление Правительства Российской Федерации «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» от 03.03.2012 г. № 171 14. Постановление Правительства РФ от 03.11.1994 № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» 15. Постановления Правительства РФ «Об утверждении Положения о порядке обращения с документами для служебного пользования» (взамен утратившего силу постановления Правительства Российской Федерации от 3

	ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» (проект) 16. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных. Приказ ФСТЭК России от 18.02.2013 г. №21 17. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11.02.2013 года № 17 18. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Приказ Гостехкомиссии от 30 августа 2002 г. №282 19. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г. 20. ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения» 21. ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества» 22. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» 23. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (взамен ГОСТ Р 51275-96) 24. ГОСТ Р 52863-2007 «Защита информации. Автоматизированные системы в защищённом исполнении. Испытания на устойчивость к намеренным силовым электромагнитным воздействиям. Общие требования» 25. ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения» 26. ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний» 27. Постановление Правительства Калининградской области от 24 января 2022 г. №26 «Об утверждении инструкции о порядке обращения со служебной информацией ограниченного распространения в Правительстве Калининградской области»
Ознакомление с лекционным материалом и контрольные вопросы к нему	Текстовые файлы, презентации и иной контент, расположенный на сайте КГ НИЦ в разделе «Обучение» - «Система дистанционного обучения».
Практические задания учитывают специфику выполняемых	Методические разработки, позволяющие индивидуализировать задания различные варианты ИСПДн в зависимости от их уровней защищенности. Такие задания представляют собой

функциональных обязанностей слушателей по своему профессиональному предназначению, в том числе рассматривают комплект документов по обработке персо-	проблемные ситуационные варианты, различающиеся моделями информационных систем персональных данных, и набором конкретных действий, существенных для определенных категорий обучаемых. Теоретический и тестовый материал размещены на сайте системы дистанционного обучения КГ НИЦ https://sdo.kgnic.ru

нальных данных, подготовленный в период самостоятельной работы	***8.2.2 Список основной литературы*** 1. Белов Е.Б. Основы информационной безопасности: Учебн. пособие Белов Е.Б., Лось В.П, Мещеряков Р.В, Шелупанов А.А. - М.: Горячая линия Телеком, 2006. - 544 с. 2. Бузов Г .А. Защита от утечки информации по техническим каналам ‘ Учебн. пособие / БузовГ.А, Калинин СВ., Кондратьев А.В.- М.: Горячая линия - Телеком, 2005. - 416 с. 3. Запечников С.В. Информационная безопасность открытых систем. Часть 1: Учебник для вузов / Запечников СВ., Милославская Н.Г, Толстой А.И, Ушаков Д.В. - М.: Горячая линия - Телеком, 2006. - 686 с. 4. Малюк А.А. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов / Малюк А.А, Пазизин СВ., Погожин Н.С. - М.: Горячая линия - Телеком, 2004. - 147 с. 5. Снытников А.А. Лицензирование и сертификация в области защиты! информации. - М.: Гелиос АРВ, 2003. - 192 с. 6. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - Минск, 2005. - 304 с. 7. Хорев А.А. Защита информации от утечки по техническим каналам: Учебн. пособие. - М.: МО РФ, 2006 8. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. - Ростов-на- Дону: Издательство СКНЦ ВШ, 2006 9. Язов Ю.К. Основы технологий проектирования систем защиты информации в информационно-телекоммуникационных системах: Монография / Аграновский А.В, Мамай В.И, Назаров И.Г., Язов Ю.К. - Издательство СКНЦВШ, 2006 10. Будников С.А, Паршин Н.В. Информационная безопасность автоматизированных систем: Учебное пособие, издание второе, дополненное - Издательство им. Е.А.Болховитинова, Воронеж, 2011 11. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. - С.-П., 2004.- 384 с. 12. Петраков А.В. Основы практической защиты информации. Учебное пособие. - М, 2005,- 281 с. 13. Девянин П.Н., Садердинов А.А, Трайнев В.А. и др. Учебное пособие. Информационная безопасность предприятия. – М., 2006.- 335 с. 14. Хорев А. А. Защита информации от утечки по техническим каналам: учеб. пособие. / А. А. Хорев. - Москва: МО РФ, 2006. – 436 с. 15. Зайцев А. П. Техническая защита информации: учебник для вузов / А. П. Зайцев [и др.]. - 5-е изд., перераб. и доп. - Москва: Горячая линия-Телеком, 2009. - 616 с. 16. Назаров, Д. М. Основы обеспечения безопасности персональных данных в организации [Текст] : учеб. пособие / Д. М. Назаров, К. М. Саматов ; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. —

Екатеринбург : Изд-во Урал. гос. экон. ун-та, 2019 — 118 с.

8.2.3 Список дополнительной литературы

1. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: учебное пособие/ Воробьев Е.Г.— Электрон. текстовые данные. — СПб.: Интермедия, 2017 — 432 с.— Режим доступа: http://www.iprbookshop.ru/66796.html — ЭБС «IPRbooks».

2. Обеспечение безопасности персональных данных [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 121с. — Режим доступа: http://www.iprbookshop.ru/52153.html — ЭБС «IPRbooks».

3. Персональные данные в государственных информационных ресурсах [Электронный ресурс]/ М.Ю. Брауде-Золотарёв [и др.] — Электрон. текстовые данные.— М.: Дело, 2016.— 55 с.— Режим доступа: http://www.iprbookshop.ru/51053.html — ЭБС «IPRbooks».

4. Правовые основы организации защиты персональных данных [Электронный ресурс]: учебное пособие/ Исаев А.С., Хлюпина Е.А.— Электрон. текстовые данные — СПб.: Университет ИТМО, 2014 — 106с. — Режим доступа: http://www.iprbookshop.ru/67564.html — ЭБС «IPRbooks».

5. Информационная безопасность для работников бюджетной сферы. Защита персональных данных [Электронный ресурс]: учебное пособие/ Шубинский М.И.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2013.— 77 с.— Режим доступа: http://www.iprbookshop.ru/68654.html — ЭБС «IPRbooks».

6. Организационно-распорядительные документы органов власти, муниципальных образований и предприятий по защите персональных данных [Электронный ресурс]: учебное пособие/ Катаржнов А.Д.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2016.— 136 с.— Режим доступа: http://www.iprbookshop.ru/67450.html — ЭБС «IPRbooks»

7. Организация защиты персональных данных [Электронный ресурс]: лабораторный практикум/ Макаров А.М., Калиберда И.В., Бондаренко К.О.— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2015.— 92 с. — Режим доступа: http://www.iprbookshop.ru/62971.html — ЭБС «IPRbooks»

8. Защита персональных данных в информационных системах [Электронный ресурс]: лабораторный практикум/ Петренко В.И., Мандрица И.В.— Электрон. текстовые данные — Ставрополь: Северо-Кавказский федеральный университет, 2018.— 118 с.— Режим доступа: http://www.iprbookshop.ru/83198.html — ЭБС «IPRbooks»

9. Персональные данные в государственных информационных ресурсах [Электронный ресурс]/ М.Ю. Брауде-Золотарёв [и др.].— Электрон. текстовые данные.— М.: Дело, 2016.— 55 с.— Режим доступа:

	http://www.iprbookshop.ru/51053.html — ЭБС «IPRbooks» 10. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена заместителем директора ФСТЭК России 15.02.2008 г.) [Электронный ресурс]. — Режим доступа: https://fstec.ru/component/attachments/download/289 11. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена заместителем директора ФСТЭК России 14.02.2008 г.). [Электронный ресурс]. — Режим доступа: https://fstec.ru/component/attachments/download/290

Информационное сопровождение	
Электронные образовательные ресурсы	Электронные информационные ресурсы
Электронно-библиотечная система «КнигаФонд – URL: http://www.knigafundt.ru	Официальный сайт Федеральной службы по техническому и экспортному контролю – URL: http://fstec.ru
Электронно-библиотечная система «IPRbooks» – URL: http://www.iprbookshop.ru	Официальный сайт Федеральной службы безопасности – URL: http://www.fsb.ru
Система дистанционного обучения КГ НИЦ https://sdo.kgnic.ru	Официальный сайт Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций – URL: http://rkn.gov.ru
	Справочная правовая система «Консультант Плюс» – URL: http://www.consultant.ru
	Информационно-правовое обеспечение «Гарант» – URL: http://www.garant.ru

8.3 Материально-технические условия реализации программы

Вид занятий	Наименование оборудования, программного обеспечения
Лекции, практические занятия	операционная система Microsoft Windows;
	пакет офисных программ Microsoft Office;
	программное обеспечения для чтения файлов в формате PDF;
	система дистанционного обучения КГ НИЦ https://sdo.kgnic.ru
	виртуальная обучающая среда Moodle