ЧАСТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «УДЦ ЗНАНИЯ ПЛЮС»

РАССМОТРЕНО
На заседании педагогического совета
Протокол № 1 от 13 января 2021 г.

УТВЕРЖДАЮ
Директор
Р.Ф.Галиакберов

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Защита информации и защита персональных данных»

72 академических часа

г. Стерлитамак

Содержание

1. Пояснительная записка

Дополнительная профессиональная программа повышения квалификации **«Защита информации и защита персональных данных»** (далее - Программа) разработана специалистами ЧУ ДПО "УДЦ "Знания Плюс" в соответствии с нормами Федерального закона от 29 декабря 2012 г. N 273-ФЗ "Об образовании в Российской Федерации", с учетом требований приказа Минобрнауки России от 1 июля 2013 г. N 499 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам", Постановления Минтруда РФ от 21.08.1998 N 37 "Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих", Приказа Министерства труда и социальной защиты РФ от 15 сентября 2016 г. N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах", Приказа Минобрнауки России от 01.12.2016 N 1515 "Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата)" с учетом требований Федерального закона от 28.12.2010 № 390-ФЗ «О безопасности», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»..

Повышение квалификации, осуществляемое в соответствии с программой (далее - обучение), проводится в соответствии с учебным планом в очной, очно-заочной, заочной формах обучения с применением электронного обучения и/или дистанционных образовательных технологий.

Разделы, включенные в учебный план программы, используются для последующей разработки календарного учебного графика, рабочих программ учебных предметов, оценочных материалов, учебно-методического обеспечения программы, иных видов учебной деятельности обучающихся и форм аттестации. Программа разработана с учетом актуальных положений законодательства об образовании и законодательства о защите информации и защите персональных данных.

Срок освоения программы составляет 72 академических часа.

Цель реализации программы: совершенствование профессиональных компетенций, необходимых для профессиональной деятельности и повышение профессионального уровня в рамках имеющейся квалификации в области защиты информации и защиты персональных данных; освоение специалистами актуальных изменений в вопросах профессиональной деятельности,

обновление их теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации.

Задачами освоения программы повышения квалификации являются:

- изучение нормативных правовых и организационных основ обеспечения безопасности информации и защиты персональных данных в информационных системах персональных данных;
- изучение методов и процедур выявления угроз безопасности информации и персональных данных в информационных системах персональных данных и оценки степени их опасности;
- практическая отработка способов и порядка проведения работ по обеспечению безопасности информации и защиты персональных данных при их обработке в информационных системах персональных данных.

В соответствии с гл.4 ст. 76 Федерального закона «Об образовании в Российской Федерации № 273-ФЗ от 29.12.2012 г., содержание дополнительной профессиональной программы повышения квалификации «Защита информации и защита персональных данных» учитывает профессиональный стандарт «Специалист по защите информации в автоматизированных системах».

Наименование выбранного профессионального стандарта: Специалист по защите информации в автоматизированных системах.

Основная цель вида профессиональной деятельности: обеспечение безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите.

Наименование обобщенной трудовой функции: обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации.

Обучающимися по программе могут быть лица, имеющие высшее или среднее

профессиональное образование; лица, получающие среднее профессиональное или высшее образование.

Наличие указанного образования должно подтверждаться документом государственного или установленного образца.

При освоении дополнительной профессиональной программы параллельно с получением среднего профессионального образования и (или) высшего образования удостоверение о повышении квалификации и выдается одновременно с получением соответствующего документа об образовании и о квалификации. Факт обучения в организации высшего или среднего профессионального образования подтверждается справкой соответствующей организации.

2. Цель и планируемые результаты обучения. Профессиональные компетенции

Целью обучения слушателей по программе является совершенствование профессиональных компетенций, необходимых для профессиональной деятельности и повышение профессионального уровня в рамках имеющейся квалификации в области защиты информации и защиты персональных данных; освоение актуальных изменений в вопросах профессиональной деятельности, обновление их теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации.

Результатом обучения слушателей по программе является повышение уровня их профессиональных компетенций за счет актуализации знаний и умений в области защиты информации и защиты персональных данных.

В процессе обучения слушатели совершенствуют свои **профессиональные компетенции** в области обеспечения защиты информации и защиты персональных данных, а также получают новые компетенции, необходимые для выполнения нового вида профессиональной деятельности *(согласно федеральному государственному образовательному стандарту высшего образования – 10.03.01 «Информационная безопасность» (уровень бакалавриата), Приказ Минобрнауки России от 01.12.2016 N 1515):*

- способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);
- способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);
- способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);
- способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);
- способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13).

Карта компетенции раскрывает компонентный состав компетенции, технологии ее формирования и оценки:

1) Дисциплинарная карта компетенции ПК 2.

ПК 2. Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
Технологии формирования:	Средства и технологии оценки:
Лекции, практическая, самостоятельная работа	Итоговая аттестация

2) Дисциплинарная карта компетенции ПК 4.

ПК 4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Технологии формирования:	Средства и технологии оценки:
Лекции, практическая, самостоятельная работа	Итоговая аттестация

3) Дисциплинарная карта компетенции ПК 5.

ПК 5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
Технологии формирования:	Средства и технологии оценки:
Лекции, практическая, самостоятельная работа	Итоговая аттестация

4) Дисциплинарная карта компетенции ПК 8.

ПК 8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	
Технологии формирования:	Средства и технологии оценки:
Лекции, практическая, самостоятельная работа	Итоговая аттестация

5) Дисциплинарная карта компетенции ПК 13.

ПК 13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
Технологии формирования:	Средства и технологии оценки:
Лекции, практическая, самостоятельная работа	Итоговая аттестация

В результате реализации программы обучаемые должны:

быть ознакомлены:

с нормативными правовыми и организационными основами защиты информации и обеспечения безопасности персональных данных в Российской Федерации; с порядком организации и проведения лицензирования деятельности в области защиты информации; с документами национальной системы стандартизации, действующими в области защиты информации;

знать:

содержание основных 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 мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

уметь:

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

иметь навык:

определения уровня защиты персональных данных; выявления угроз безопасности персональных данных в информационных системах персональных данных.

3. Учебный план
дополнительной профессиональной программы повышения квалификации
«Защита информации и защита персональных данных»

Учебный план Программы определяет перечень, последовательность, общую трудоемкость дисциплин и формы контроля знаний.

Образовательная деятельность слушателей предусматривает следующие виды учебных занятий и учебных работ:

- лекции;

- практические, самостоятельные работы;

- итоговая аттестация (экзамен в форме тестирования).

Направление подготовки: Информационная безопасность

Категория слушателей: лица, имеющие высшее или среднее профессиональное образование; лица, получающие высшее или среднее профессиональное образование

Общая трудоемкость программы: 72 академических часа

Форма обучения: очная, очно-заочная, заочная с применением дистанционных образовательных технологий и/или электронного обучения

Выдаваемый документ: удостоверение о повышении квалификации

№ п/п	Разделы курса	Всего часов на курс обучения	в том числе	
			лекции	СРС*, практические занятия
1	Общие вопросы технической защиты информации	24	8	16
2	Организация обеспечения безопасности персональных данных в информационных системах персональных данных	46	16	30
	Итоговая аттестация(экзамен)	2	-	2
	Итого:	**72**	**24**	**48**

* СРС – самостоятельная работа слушателей

Учебно-тематический план

дополнительной профессиональной программы повышения квалификации

«Защита информации и защита персональных данных»

№ п/п	Разделы и темы курса	Всего часов на курс обучения	в том числе	
			лекции	СРС*, практические занятия
1	**Раздел 1. Общие вопросы технической защиты информации**	**24**	**8**	**16**
1.1.	Тема 1. Основные понятия и определения	8	2	6
1.2.	Тема 2. Нормативно-правовое обеспечение защиты персональных данных	16	6	10
2	**Раздел 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных**	**46**	**16**	**30**
2.1.	Тема 1. Угрозы и уязвимости безопасности персональных данных в информационных системах персональных данных	24	8	16
2.2.	Тема 2. Организационные и технические мероприятия по защите персональных данных в информационных системах	22	8	14
	Итоговая аттестация(экзамен)	2	-	2
	Итого:	**72**	**24**	**48**

* СРС – самостоятельная работа слушателей

4. Календарный учебный график

Календарный учебный график представляет собой график учебного процесса, устанавливающий последовательность и продолжительность обучения и итоговой аттестации по учебным дням.

Порядковый номер дня обучения	Наименование тем курса	Количество часов
	Раздел 1. Общие вопросы технической защиты информации	
1-ый	Тема 1. Основные понятия и определения	8
2-ой	Тема 2. Нормативно-правовое обеспечение защиты персональных данных	8
3-ий	Тема 2. Нормативно-правовое обеспечение защиты персональных данных	8
	Раздел 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных	
4-ый	Тема 1. Угрозы и уязвимости безопасности персональных данных в информационных системах персональных данных	8
5-ый	Тема 1. Угрозы и уязвимости безопасности персональных данных в информационных системах персональных данных	8
6-ой	Тема 1. Угрозы и уязвимости безопасности персональных данных в информационных системах персональных данных	8
7-ой	Тема 2. Организационные и технические мероприятия по защите персональных данных в информационных системах	8
8-ой	Тема 2. Организационные и технические мероприятия по защите персональных данных в информационных системах	8
9-ый	Тема 2. Организационные и технические мероприятия по защите персональных данных в информационных системах Итоговая аттестация	6 2

5. Рабочая программа

Раздел 1. Общие вопросы технической защиты информации

Тема 1. Основные понятия и определения

Основные понятия в области технической защиты информации (ТЗИ). Стратегия национальной безопасности Российской Федерации. 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.

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 сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP. 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.

Тема 2. Нормативно-правовое обеспечение защиты персональных данных

Международное и национальное право в области защиты персональных данных.

Федеральное законодательство Российской Федерации в области защиты персональных данных.

Содержание и основные положения Федерального Закона Российской Федерации «О персональных данных» № 152-ФЗ.

Специальные нормативные документы по технической защите сведений конфиденциального характера.

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.

Раздел 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных

Тема 1. Угрозы и уязвимости безопасности персональных данных в информационных системах персональных данных

Угрозы и уязвимости безопасности персональных данных при их обработке в

информационных системах. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных.

Наиболее часто реализуемые угрозы. Особенности информационного элемента информационной системы персональных данных.

Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, 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 система персональных данных. Общий порядок организации обеспечения безопасности персональных данных. 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 защищенности информации, обрабатываемой основными техническими средствами и системы их коммуникации.

Методология формирования модели угроз с использованием Методических рекомендаций ФСБ.

Тема 2. Организационные и технические мероприятия по защите персональных данных в информационных системах

Порядок организации защиты персональных данных. 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.

Меры по обеспечению безопасности 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.

Построение системы защиты 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.

Итоговая аттестация – 2 часа

6. Организационно-педагогические условия реализации Программы

Организационно-педагогические условия, созданные в организации, являются результатом целенаправленной деятельности педагогического коллектива по созданию комфортной образовательной среды в организации.

Образовательная организация обеспечивает:

- наличие на праве собственности или ином законном основании зданий, строений, сооружений, помещений и территорий, необходимых для осуществления образовательной деятельности;

- наличие материально-технического обеспечения образовательной деятельности, оборудование помещений в соответствии с государственными и местными нормами и требованиями;

- наличие санитарно-эпидемиологического заключения о соответствии санитарным правилам зданий, строений, сооружений, помещений, оборудования и иного имущества, которые используются для осуществления образовательной деятельности;

- наличие условий для функционирования электронной информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий и соответствующих технологических средств и обеспечивающей освоение обучающимися независимо от их местонахождения образовательной программы в полном объеме;

- наличие электронных образовательных и информационных ресурсов по программе, соответствующих установленным требованиям;

- наличие в штате или привлечение на ином законном основании педагогических работников, имеющих профессиональное образование, обладающих соответствующей квалификацией, имеющих стаж работы, необходимый для осуществления образовательной деятельности по программе;

- неразглашение персональных данных слушателей третьим лицам при обработке персональных данных;

- наличие лицензии на осуществление образовательной деятельности по реализации дополнительных профессиональных программ.

Материально-техническое обеспечение образовательного процесса

Образовательная организация полностью обеспечена материально-технической базой для проведения обучения слушателей Программы. В наличии оборудованные современными

техническими средствами обучения учебные аудитории для проведения теоретических и практических занятий.

Учебные аудитории оснащены компьютерной и оргтехникой, проекционно-демонстрационным оборудованием, специализированными демонстрационными средствами для реализации Программы.

Реализация Программы обеспечена соответствующей учебно-методической документацией по всем темам, представленной в виде электронных учебных пособий.

Реализация программы обеспечивается доступом каждого обучающегося к базам данных и библиотечным фондам, формируемым по полному перечню тем. Во время самостоятельной подготовки обучающиеся обеспечены доступом в сеть Интернет. Каждый обучающийся обеспечен не менее чем одним учебным печатным или электронным изданием по каждой теме.

Нормативные условия.

Режим работы организации. Продолжительность учебного года - 52 учебные недели (полный календарный год). Итоговая аттестация обучающихся курсов проводится в сроки, установленные учебной программой. Дата итоговой аттестации устанавливается приказом по организации. Продолжительность учебного занятия (академический час) – 45 минут. Учебные занятия поводятся с понедельника по пятницу с 8 до 19 часов, согласно расписанию. Суббота, воскресенье – выходные дни. Объем максимально допустимой нагрузки в течение дня – 8 академических часов. Наполняемость учебной группы – от 2 до 40 человек.

Организационные условия.

Формы и способы организации обучения.

В зависимости от конкретных целей планируется применять в учебном процессе следующие формы организации обучения:

• Лекция

Лекция предполагает устное изложение учебного материала, отличающееся большой емкостью, чем рассказ, большой сложностью логических построений, образов, доказательств и обобщений. Лекция, как правило, занимает все занятие, в то время как рассказ занимает лишь его часть.

В ходе лекции используются приемы устного изложения информации, поддержания внимания в течение длительного времени, активизации мышления слушателей, приемы обеспечения логического запоминания, убеждения, аргументации, доказательства, классификации, систематизации и обобщения и др.

Условиями эффективного проведения лекции является четкое продумывание и сообщение плана лекции, логически стройное и последовательное изложение одного за другим всех пунктов

плана с резюме и выводами после каждого из них и логическими связями при переходе к следующему разделу. Не менее важно обеспечить доступность, ясность изложения, объяснить термины, подобрать примеры и иллюстрации, подобрать средства наглядности. Лекцию читают в таком темпе, чтобы слушатели могли сделать необходимые записи. Преподаватели поэтому четко выделять то, что следует записать, однозначно повторять при необходимости, чтобы облегчить записи.

Лекция - вид устного изложения учебного материала и обучающего взаимодействия преподавателя с обучающимися. Она предполагает использование в разнообразных пропорциях и изложения фактов, и краткого вспомогательного диалога, обеспечивающего диагностику получаемой преподавателем обратной информации о качестве восприятия и усвоения материала слушателями.

Лекция активизирует познавательную деятельность обучающихся, будит их мысль, приводит к размышлениям над проблемами изучаемой дисциплины, к поискам ответов на возникшие ы.

Подобной формой можно также пользоваться при проведении вебинаров.

• Вебинар

Вебинар (от англ. «webinar», сокр. от «Web-based seminar») или online-семинар – это новая форма дистанционного обучения посредством Интернет–вещания. Проводится вебинар на специальной Интернет–площадке с удаленным доступом неограниченного количества участников. Преимущества этого метода обучения – снижение расходов Заказчика на обучение, так как практически отсутствуют расходы на проезд слушателей к месту обучения и обратно. При этом обучающие ресурсы вебинара совпадают с очным обучением. Участники видят ведущего, могут задавать ему ы (письменно или устно), комментировать высказывания других участников вебинара, просматривать слайды презентации, скачивать все предлагаемые ведущим материалы и даже выполнять практические и контрольные задания.

Характеристика кадрового состава организации.

Педагогический коллектив организации укомплектован педагогическими кадрами в полном объеме, 100% педагогических работников имеют высшее образование, все педагогические работники организации прошли обучение по преподаваемым предметам.

Педагогические работники организации постоянно повышают свой профессиональный уровень, изучают все изменения в законодательстве Российской Федерации, связанные с преподаванием соответствующих предметов.

Возможно, при необходимости, привлечение к образовательному процессу

высококвалифицированных специалистов из числа руководителей и ведущих специалистов государственных органов, учреждений, а также преподавателей ведущих российских и иностранных образовательных организаций.

7. Формы аттестации и оценочные материалы

Освоение Программы завершается итоговой аттестацией слушателей в форме тестирования.

Лицам, успешно освоившим Программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца.

Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть Программы и (или) отчисленным из образовательной организации, выдается справка об обучении или о периоде обучения.

Перечень примерных тестовых вопросов для проведения итоговой аттестации

1. Автоматизированная обработка персональных данных – это …

1. Обработка персональных данных с использованием средств автоматизации
2. Обработка персональных данных с помощью средств вычислительной техники
3. Обработка персональных данных пользователя с применением компьютера

2. Информация – это …

1. Любые данные, представленные на материальном носителе
2. Сведения, принадлежащие кому-либо и защищаемые законом
3. Сведения (сообщения, данные), независимо от формы их представления

3. Информационная система персональных данных – это …

1. Информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств
2. Пользователь, средства автоматизации, базы данных
3. Контролируемое пространство, в котором происходит обработка персональных данных

4. Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

4. Безопасность персональных данных – это …

1. Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных
2. Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность персональных данных
3. Состояние защищенности персональных данных, характеризуемое способностью технических средств обеспечить конфиденциальность персональных данных

5. Блокирование персональных данных – это …

1. Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
2. Временное прекращение обработки персональных данных
3. Временное прекращение обработки персональных данных для уточнения персональных данных

6. Доступ к информации – это …

1. Возможность получения информации и ее использования
2. Возможность использования информации
3. Возможность доступа к информации
4. Возможность доступа к информации, но не ее использования

7. Целью Федерального закона от 27.07.2006 № 152-ФЗ является:

1. Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну
2. Контроль за обработкой персональных данных операторами персональных данных
3. Соответствие законодательства РФ в сфере персональных данных Конвенции Совета Европы от 1981года

8. Защищаемая информация – это …

1. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации
2. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации
3. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов
4. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями Федерального закона «О защищаемой информации в Российской Федерации»

9. Идентификация – это …

1. Присвоение субъектам и объектам доступа идентификатора и сравнение предъявляемого идентификатора с вводимым идентификатором
2. Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
3. Присвоение субъектам и объектам доступа идентификатора
4. Присвоение субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с вводимым идентификатором

10. Информационные технологии – это …

1. Средства поиска, сбора, хранения, обработки, предоставления, распространения информации
2. Методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких методов
3. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
4. Процессы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов

11. Что понимается под понятием «Конфиденциальность персональных данных»?

1. Обязательное для соблюдения оператором или иным лицом требование не допускать их распространения без согласия субъекта персональных данных
2. Обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотренное федеральным законом
3. Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания

12. Материальный носитель (носитель информации) – это…

1. Любой материальный объект, используемый для хранения или передачи информации
2. Любой материальный объект, используемый для хранения информации
3. Любой материальный субъект, используемый для хранения или передачи информации

13. Межсетевой экран – это …

1. Функционально-распределенное программно-аппаратное средство, реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы
2. Локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы
3. Локальное программное средство, реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы

14. Нарушитель безопасности персональных данных – это …

1. Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных
2. Физическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных

3. Физическое или юридическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных

15. Недекларированные возможности – это …

1. Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации
2. Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых появляются новые возможности для работы
3. Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации

16. Общедоступные персональные данные – это …

1. Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных
2. Персональные данные, доступ неограниченного круга лиц к которым предоставлен в соответствии с федеральными законами
3. Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности

17. Правила разграничения доступа – это …

1. Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа
2. Совокупность правил для обеспечения информационной безопасности в организации
3. Совокупность правил, для объектов доступа

18. Специальные категории персональных данных – это …

1. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и судимости
2. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных убеждений, интимной и личной жизни жизни
3. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, состояния здоровья, интимной жизни
4. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и судимости

19. Трансграничная передача персональных данных – это …

1. Передача персональных данных на территорию иностранного государства
2. Передача персональных данных на территорию другого субъекта РФ органу власти данного субъекта, физическому лицу или юридическому лицу данного субъекта РФ
3. Передача персональных данных на территорию иностранного государства или органу власти иностранного государства
4. Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

20. **Целостность информации – это ...**

1. Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения)
2. Состояние информации, при котором отсутствует любое ее изменение
3. Состояние информации, при котором изменение осуществляется только преднамеренно субъектами, имеющими на него право
4. Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

21. Что такое персональные данные?

1. Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
2. Информация о частной жизни физического лица, доступ к которой он решил ограничить
3. Сведения о религиозных убеждениях, политических взглядов, расовой и национальной принадлежности субъекта персональных данных
4. Любые сведения независимо от формы их представления

22. Оператор персональных данных — это …

1. Государственный орган, осуществляющий автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке
2. Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными
3. Юридическое лицо, осуществляющее автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке
4. Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, но не определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

23. Обработка персональных данных – это …

1. Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение(обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных)
2. Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление,

доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, осуществляемые с помощью средств вычислительной техники

3. Чтение, запись, сортировка, модификация, передача персональных данных в информационной системе

24. Распространение персональных данных – это …

1. Действия, направленные на раскрытие персональных данных неопределенному кругу лиц
2. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
3. Передача персональных данных оператору персональных данных

25. Предоставление персональных данных – это …

1. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
2. Действия, направленные на раскрытие персональных данных по мотивированному запросу
3. Нет правильного ответа

26. Уничтожение персональных данных – это …

1. Действия, в результате которых становится невозможно определить субъекта персональных данных в информационной системе персональных данных
2. Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных
3. Удаление персональных данных из информационной системы персональных данных
4. Действия, направленные на уничтожение носителей персональных данных

27. Обезличивание персональных данных – действия, в результате которых…

1. Невозможно распространять персональные данные
2. Невозможно выполнять сбор персональных данных
3. Выполняется уничтожение персональных данных в информационной системе
4. Становится невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

28. Что понимается под понятием «Контролируемая зона»?

1. Пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств
2. Пространство, в котором не исключается неконтролируемое пребывание сотрудников и посетителей оператора, но исключается неконтролируемое пребывание посторонних транспортных, технических и иных материальных средств
3. Пространство, в котором не исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств

29. Что такое биометрические персональные данные?

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта персональных данных
2. Сведения, которые характеризуют физиологические особенности человека, на основании которых можно установить его личность
3. Сведения, которые характеризуют биологические особенности человека, на основании которых можно установить его личность

30. Как расшифровывается аббревиатура «НСД» применительно к защите информации?

1. Национальные скоростные дороги
2. Несанкционированный доступ
3. Национальный союз дзюдо
4. Национально-социалистическое движение

31. Как расшифровывается аббревиатура «НДВ» применительно к защите информации?

1. Норматив допустимого воздействия
2. Недекларированная возможность
3. Небо для всех
4. Национальный директор по вооружению

32. Какое из свойств защищаемой информации не является основным?

1. Целостность
2. Регистрируемость
3. Доступность
4. Конфиденциальность

33. Законодательство Российской Федерации в области персональных данных состоит из:

1. Федерального закона «О Государственной тайне»
2. Федерального закона «Об электронной цифровой подписи»
3. Федерального закона «О персональных данных»
4. Федеральных законов, Постановлений Правительства и нормативно-правовых актов уполномоченных органов государственной власти РФ в сфере информации и персональных данных

34. Дата официального опубликования Федерального закона «О персональных данных»:

1. 26 июня 2006 года
2. 26 июля 2007 года
3. 27 июля 2006 года
4. 27 июня 2007 года

35. Целью Федерального закона «О персональных данных» является:

1. Обеспечение защиты информации в Российской Федерации
2. Осуществление права на поиск, получение, передачу, производство и распространение информации
3. Обеспечение защиты персональных данных
4. Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных

36. На какие отношения не распространяется действие Федерального закона "О персональных данных"?

1. На отношения, возникающие при обработке персональных данных физическими лицами, исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных
2. На отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну
3. Не распространяется на оба перечисленных варианта

37. Оператор персональных данных – это .. (Несколько вариантов ответа):

1. Физическое лицо
2. Юридическое лицо
3. Муниципальный орган
4. Государственный орган
5. Гражданин
6. Государственный служащий

38. Перед кем оператор персональных данных несет ответственность?

1. Перед субъектом персональных данных
2. Перед Роскомнадзором
3. Не перед кем не несет ответственности

39. На какие отношения распространяется действие Федерального закона «О персональных данных»?

1. На отношения, возникающие при обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных
2. На отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну
3. На отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами
4. Распространяется на все перечисленные варианты

40. В какой орган нужно отправить Уведомление об обработке персональных данных?

1. Администрация города или района
2. Департамент информационных технологий
3. Управление Роскомнадзора

41. Оператор при сборе персональных данных через свой официальный сайт обязан в соответствии с ч.2 ст.18.1 152-ФЗ на сайте опубликовать документы:

1. Форму согласия на обработку персональных данных
2. Положение о защите персональных данных
3. Документы, определяющие политику в отношении обработки персональных данных

42. Управление Роскомнадзора уведомляет оператора персональных данных о проведении внеплановой проверки:

1. Не менее чем за 24 часа до начала ее проведения любым доступным способом
2. Не менее чем за 3 дня до начала ее проведения любым доступным способом
3. Не менее чем за 24 часа до начала ее проведения только в письменном виде

43. Срок проведения плановой проверки не может превышать:

1. 35 рабочих дней
2. 28 рабочих дней
3. 20 рабочих дней
4. Срок проведения проверок не ограничен

44. В течение какого времени со дня получения запроса Оператор обязан предоставить в Управление Роскомнадзора необходимую информацию?

1. В течение 30 дней
2. В течение двух рабочих дней
3. В течение 5 рабочих дней
4. Срок предоставления документов не ограничен

45. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных, оператор обязан прекратить обработку персональных данных, и, если

сохранение персональных данных более не требуется для целей обработки, уничтожить персональных данных в срок, не превышающий с даты поступления указанного отзыва:

1. 30 рабочих дней
2. 30 календарных дней
3. 20 календарных дней
4. 10 рабочих дней

46. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором, оператор обязан прекратить неправомерную обработку персональных данных с даты этого выявления в срок, не превышающий:

1. 5 рабочих дней
2. 7 рабочих дней
3. 10 рабочих дней
4. 30 календарных дней

47. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных и уничтожить соответствующие персональных данных в срок, не превышающий с даты достижения цели обработки персональных данных:

1. 10 дней
2. 30 дней
3. 7 дней

48. Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных:

1. В течение 3 рабочих дней после начала обработки персональных данных
2. В течение 4 рабочих дней после начала обработки персональных данных
3. До начала обработки персональных данных
4. В течение 7 рабочих дней после начала обработки персональных данных

49. Если персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные в срок, не превышающий:

1. 7 рабочих дней
2. 10 рабочих дней

3. 15 календарных дней
4. 30 рабочих дней

50. Управление Роскомнадзора уведомляет о проведении плановой проверки:

1. Не позднее, чем в течение 3-х рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Управления Роскомнадзора с уведомлением о вручении или иным доступным способом
2. Не позднее, чем в течение 7-ми рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Управления Роскомнадзора с уведомлением о вручении или иным доступным способом
3. Не менее чем за 24 часа до начала ее проведения любым доступным способом
4. Предварительное уведомление Оператора о начале проведения плановой проверки не требуется

51. Контроль за выполнением требований Постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» проводится не реже 1 раза в:

1. 5 лет
2. 3 года
3. 1 год

52. Основная статья, по которой предусмотрена ответственность для Оператора по результатам проверки:

1. УК РФ. Статья 137. Нарушение неприкосновенности частной жизни
2. КоАП. Статья 19.5. Невыполнение в срок законного предписания
3. КоАП. Статья 19.7. Непредставление сведений (информации)
4. КоАП. Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

53. Кто должен осуществлять внутренний контроль за соблюдением оператором законодательства Российской Федерации о персональных данных?

1. Администратор безопасности использования персональных данных
2. Ответственный за организацию обработки персональных данных
3. Ответственный за обеспечение безопасности персональных данных

4. Руководитель организации

54. Какие меры по обеспечению безопасности персональных данных при неавтоматизированной обработке являются обязательными в соответствии с постановлением Правительства РФ от 15.09.2008г. № 687?

1. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации
2. Использование средств контроля и управлении доступом
3. Использование запираемых шкафов, сейфов и решеток на окнах
4. Должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, устанавливаются оператором.

55. Какая ответственность предусмотрена за нарушение законодательства РФ о персональных данных?

1. Дисциплинарная
2. Административная
3. Уголовная
4. Все перечисленные

56. Рекомендуемые Роскомнадзором методы обезличивания персональных данных:

1. Метод введения идентификаторов; метод маскирования; метод перемешивания; метод замены состава или семантики
2. Метод введения идентификаторов; метод абстрагирования; метод перемешивания; метод разделения состава или семантики
3. Метод введения идентификаторов; метод декомпозиции; метод перемешивания; метод изменения состава или семантики

57. В соответствии с каким законодательным актом технические задания на создание информационных систем для ГИС и МИС обязательно выполнять в соответствии с ГОСТ 34.602-89, ГОСТ 5183-2000, ГОСТ Р 51624-2000, ГОСТ 34.601-90, ГОСТ 34.201-89?

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

2. Приказ ФСТЭК 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»
3. Приказ ФСТЭК России от 20.07.2012 N 89 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации»
4. Федеральный закон от 27.12. 2002 N 184-ФЗ «О техническом регулировании»

58. Сколько дней максимум может длиться проверка ФСБ?

1. 20 рабочих дней
2. 20 календарных дней
3. 30 рабочих дней
4. 30 календарных дней

59. Какой документ составляется по результатам проверки ФСБ?

1. Отчет по результатам проверки
2. Акт проверки
3. Заключение о проверке
4. Протокол

60. Как называется документ, который составляется по результатам проверки и в нем указываются нарушения, которые необходимо устранить?

1. Предписание
2. Заключение
3. Акт о выявленных нарушениях
4. акт проверки

61. Управление Роскомнадзора региона, в соответствии с постановлением Правительства РФ от 12.02.2019 г. № 146 уведомляет оператора о проведении плановой проверки за:

1. 7 календарных дней
2. 3 рабочих дня

3. 14 рабочих дней

62. Какие виды проверок бывают?

1. Документарные и выездные
2. Только документарные
3. Только выездные

63. Кто может взаимодействовать с сотрудниками Роскомнадзора при проведении выездной проверки?

1. Руководитель организации и уполномоченный сотрудник
2. Любой сотрудник
3. Только ответственный за организацию обработки персональных данных

64. Что мы получаем по итогу разработки модели угроз?

1. Перечень наиболее опасных угроз
2. Перечень наиболее вероятных угроз
3. Перечень актуальных угроз
4. Перечень неактуальных угроз

65. Какое из свойств защищаемой информации не является основным?

1. Целостность
2. Регистрируемость
3. Доступность
4. Конфиденциальность

66. Требования по защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах устанавливает:

1. Приказ ФСТЭК №21
2. Приказ ФСТЭК №17
3. Приказ ФСТЭК №58

67. Что из перечисленного не подлежит обязательному учёту?

1. Средства криптографической защиты информации

2. Материальные носители персональных данных
3. Блоки питания ПК, обрабатывающих персональные данные
4. Сотрудники, доступ которых к персональным данным обусловлен их должностными обязанностями

68. Обеспечение информационной безопасности есть обеспечение…

1. Независимости информации
2. Изменения информации
3. Копирования информации
4. Сохранности информации
5. Преобразования информации

69. Каким нормативно правовым актом Российской Федерации установлены «Правила организации и осуществления государственного контроля и надзора за обработкой персональных данных»?

1. Постановлением Правительства РФ от 13 февраля 2019 г. № 146
2. Приказом Минкомсвязи РФ от 21 января 2019 г. № 10
3. Приказом Роскомнадзора от 30 октября 2018 г. № 159

70. Перед передачей персональных данных субъекта на территорию другого государства оператор ….

1. Получает согласие на передачу персональных данных от субъекта
2. Принимает самостоятельно решение о передаче персональных данных субъекта
3. Выясняет, относится ли данная страна к государствам, обеспечивающим адекватную защиту персональных данных

71. Государственный контроль и надзор в сфере персональных данных, в соответствии с постановлением Правительства № 146 от 13.02.2019 года проводится посредством:

1. Плановых и внеплановых проверок
2. Принятия мер по пресечению и устранению выявленных нарушений
3. Проведения мероприятий по контролю без взаимодействия с операторами
4. Проведения мероприятий по профилактике нарушений
5. Проведением мероприятий по контролю за распространением персональных данных

72. Каким Федеральным законом и с какого времени контроль и надзор за обработкой персональных данных выведен из-под 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного и муниципального контроля?

1. 149-ФЗ с 1 декабря 2016 г.
2. 242-ФЗ с 1 сентября 2015 г.
3. Нет правильного ответа

73. В каком случае фотографию можно отнести к биометрическим персональным данным?

1. В случае, если копия паспорта с фотографией находится в личном деле сотрудника
2. В случае если фотография зарегистрирована в СКУД (система контроля и управления доступом, т.е. проходная завода)
3. В случае если эта фотография сделана в публичном месте
4. В случае, если гражданин проходит паспортный контроль в зелёной зоне аэропорта

74. Правила организации и осуществления государственного контроля и надзора за обработкой персональных данных в соответствии с постановлением Правительства РФ от 12.02.2019 г. № 146 определяют:

1. Порядок организации и проведения проверок операторов персональных данных
2. Порядок контроля и надзора за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии со ст.19.ФЗ-152
3. Оба ответа верны

75. Управление Роскомнадзора региона, в соответствии с постановлением Правительства РФ от 12.02.2019 г. № 146 согласует с органами прокуратуры внеплановые проверки:

1. По результатам обращения граждан, поступивших в Роскомнадзор
2. В случае неисполнения оператором предписания Роскомнадзора
3. По результатам проведения мероприятий по контролю без взаимодействия с оператором

76. При проведении проверки в отношении оператора, который осуществляет свою деятельность на территориях нескольких субъектов Российской Федерации, срок проведения проверки устанавливается отдельно по каждому филиалу, представительству оператора, при этом общий срок проведения такой проверки не может превышать...

1. 60 рабочих дней
2. 20 рабочих дней
3. 30 календарных дней

77. Основанием для продления срока проведения проверки является:

1. Получение в ходе проведения проверки от правоохранительных органов, в том числе органов прокуратуры, либо из иных источников документов, свидетельствующих о нарушении оператором требований
2. Возникновение обстоятельств непреодолимой силы (затопление, наводнение, пожар и тому подобное) на территории, где проводится проверка
3. Непредставление оператором в ходе проведения проверки необходимых документов
4. Выявление в ходе проведения проверки обстоятельств, связанных с большим объемом проверяемых и анализируемых документов, количеством осуществляемых видов деятельности по обработке персональных данных, разветвленностью организационно-хозяйственной структуры оператора, сложностью технологических процессов обработки персональных данных
5. Все ответы верны

78. Проводятся ли внеплановые документарные проверки в отношении оператора?

1. Проводятся
2. Не проводятся
3. Проводятся по согласованию с Прокуратурой

79. Проводится ли выездная проверка оператора - физического лица, не являющегося индивидуальным предпринимателем?

1. Проводится
2. Не проводится
3. Проводится по согласованию с Прокуратурой

80. К мероприятиям по контролю без взаимодействия проверяющего органа с операторами относится:

1. Наблюдение за соблюдением требований при размещении информации в сети "Интернет" и средствах массовой информации
2. Наблюдение за соблюдением требований посредством анализа информации о деятельности оператора, которая представляется оператором (в том числе посредством использования федеральных государственных информационных систем) в орган по контролю и надзору в соответствии с федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации или может быть получена (в том числе в рамках межведомственного информационного взаимодействия) органом по контролю и надзору
3. Оба ответа верны

81. В целях профилактики нарушения требований орган по контролю и надзору:

1. Размещает на своем официальном сайте в сети "Интернет" перечень нормативных правовых актов, содержащих требования

2. Осуществляет информирование операторов о положении дел в области защиты прав субъектов персональных данных
3. Обеспечивает ежегодное обобщение практики осуществления государственного контроля и надзора в области персональных данных посредством подготовки отчета о деятельности по осуществлению государственного контроля и надзора в области персональных данных
4. Размещает на своем официальном сайте в сети "Интернет" информацию о наиболее часто выявляемых в ходе осуществления контроля и надзора нарушениях требований, в результате которых оператор был привлечен к административной ответственности либо оператору было выдано предписание об устранении выявленных нарушений
5. Размещает на своем официальном сайте в сети "Интернет" руководства по соблюдению требований, информацию о проведении семинаров и конференций
6. Осуществляет разъяснительную работу в средствах массовой информации и иными способами
7. Выдает предостережения о недопустимости нарушения требований
8. Все ответы верны

82. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются …

1. Роскомнадзором
2. Оператором
3. Правительством Российской Федерации

83. Допускается ли объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой?

1. Допускается
2. Не допускается
3. Допускается с письменного разрешения Роскомнадзора

84. Обязано ли лицо, осуществляющее обработку персональных данных по поручению оператора, получать согласие субъекта персональных данных на обработку его персональных данных?

1. Обязано
2. Не обязано
3. Обязано, если обрабатываются персональные данные иностранного гражданина

85. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед…

1. Субъектом персональных данных
2. Оператором
3. Роскомнадзором

86. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается…

1. Правительством Российской Федерации
2. Оператором
3. Органом муниципальной власти

87. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают ….., если такое согласие не было дано субъектом персональных данных при его жизни.

1. Наследники субъекта персональных данных
2. Лица, знакомые с субъектом персональных данных
3. Органы ЗАГС

88. Кем может осуществляться обработка персональных данных о судимости?

1. Государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации
2. Иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами
3. Оба ответа верны

89. В каких случаях обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных?

1. В связи с реализацией международных договоров Российской Федерации о реадмиссии
2. В связи с осуществлением правосудия и исполнением судебных актов
3. В связи с проведением обязательной государственной дактилоскопической регистрации
4. В случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации
5. Во всех перечисленных случаях

90. Могут ли быть ограничены права и свободы человека и гражданина по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в

государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных?

1. Могут
2. Не могут
3. Могут, если человек (гражданин) имеет судимость

91. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе…

1. На возмещение убытков
2. На компенсацию морального вреда в судебном порядке
3. Оба ответа верны

92. Кем устанавливаются требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных?

1. Оператором
2. Роскомнадзором
3. Правительством Российской Федерации

93. Под уровнем защищенности персональных данных понимается …

1. Комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных
2. Уровень блокировки угроз несанкционированного доступа
3. Нет правильного ответа

94. Может ли оператор взимать плату за предоставление субъекту персональных данных или его представителю возможности ознакомления с персональными данными, относящимися к этому субъекту персональных данных?

1. Не может
2. Может
3. Может по тарифам, установленным Правительством Российской Федерации

95. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан…

1. Осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных
2. Уничтожить персональные данные, относящиеся к этому субъекту персональных данных
3. Нет правильного ответа

96. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение…

1. 5 рабочих дней со дня представления таких сведений
2. 10 рабочих дней со дня представления таких сведений
3. 7 рабочих дней со дня представления таких сведений

97. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1. Обрабатываемых в соответствии с трудовым законодательством
2. Включающих в себя только фамилии, имена и отчества субъектов персональных данных
3. Оба ответа верны

98. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных. В каком виде подается уведомление?

1. В виде телефонограммы
2. В виде документа на бумажном носителе или в форме электронного документа
3. Оба ответа верны

99. Лицо, ответственное за организацию обработки персональных данных, обязано:

1. Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных
2. Доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных
3. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов
4. Все ответы верны

100. Какой орган ведет реестр операторов?

1. Роскомнадзор
2. Правительство Российской Федерации
3. Реестр операторов не ведется

8. Список литературы

Нормативно-правовые и технические акты:

1. Федеральный закон от 27.12. 2002 N 184-ФЗ «О техническом регулировании» (с изменениями и дополнениями);
2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (с изменениями и дополнениями);
3. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (с изменениями и дополнениями);
4. Федеральный закон "О безопасности" от 28.12.2010 N 390-ФЗ (с изменениями и дополнениями);
5. Постановление Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
6. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
7. Постановление Правительства РФ от 13.02.2019 N 146 "Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных".

Дополнительная литература:

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 476 с.
2. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.
3. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 400 с.
4. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с.
5. Емельянова, Н.З. Защита информации в персональном компьютере: Уч.пос / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2017. - 352 с.
6. Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - М.: Риор, 2017. - 480 с.

7. Камский, В. Защита личной информации в интернете, смартфоне и компьютере / В. Камский. - СПб.: Наука и техника, 2017. - 272 с.
8. Краковский, Ю.М. Защита информации: Учебное пособие / Ю.М. Краковский. - Рн/Д: Феникс, 2015. - 416 с.
9. Краковский, Ю.М. Защита информации: учебное пособие / Ю.М. Краковский. - РнД: Феникс, 2017. - 347 с.
10. Крамаров, С.О. Криптографическая защита информации: Учебное пособие / С.О. Крамаров, Е.Н. Тищенко, С.В. Соколов и др. - М.: Риор, 2019. - 112 с.
11. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. - 230 с.
12. Мельников, В.П. Защита информации: Учебник / В.П. Мельников. - М.: Академия, 2019. - 320 с.
13. Москвитин, Г.И. Комплексная защита информации в организации / Г.И. Москвитин. - М.: Русайнс, 2017. - 400 с.
14. Северин, В.А. Правовая защита информации в коммерческих организациях / В.А. Северин. - М.: Academia, 2017. - 126 с.
15. Северин, В.А. Правовая защита информации в коммерческих организациях: Учебное пособие / В.А. Северин. - М.: Академия, 2019. - 656 с.
16. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2017. - 448 с.
17. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2018. - 352 с.

Электронные ресурсы:

1. СПС КонсультантПлюс: Законодательство: Версия Проф. – URL: https://www.consultant.ru