Частное образовательное учреждение
дополнительного профессионального образования
«Институт переподготовки и повышения квалификации»
ЧОУ ДПО «ИППК»

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

(программа повышения квалификации)

«Информационная безопасность в образовательной организации»

г.Новочеркасск
2024 г.

1. ВВЕДЕНИЕ

Учебная программа повышения квалификации специалистов в области информационной безопасности по курсу «Информационная безопасность в образовательной организации» (далее - программа) разработана с учётом 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».

Основой для разработки программы являются Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», № 149-ФЗ от 27 июля «Об информации, информационных технологиях и о защите информации», № 436-ФЗ от 29 декабря 2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию», Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом ФСТЭК России от 18.02.2013 № 21, а также документы, регламентирующие вопросы обеспечения безопасности персональных данных: «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утвержденную заместителем директора ФСТЭК России 15 февраля 2008 г., «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утвержденную заместителем директора ФСТЭК России 14 февраля 2008 г., письмо Минобрнауки России от 28.04.2014 N ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет»

При разработке программы выполнены требования к содержанию дополнительных профессиональных образовательных программ, утверждённые приказом Минобразования России от 18.06.1997 № 1221.

Цель обучения по программе: овладение слушателями актуальных изменений в вопросах профессиональной деятельности, обновление их теоретических знаний, развитие практических навыков по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации, защиту воспитанников образовательных учреждений от негативной и запрещенной информации в Интернете, организационную и методическую поддержку педагогов.

Поставленная цель достигается решением следующих задач:

– изучением правовых и организационных основ обеспечения безопасности персональных данных в информационных системах

персональных данных;

– изучением методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценки степени их опасности;

– практической отработкой способов и порядка проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

– изучением методов и процедур обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду;

– практической отработкой способов и порядка проведения работ по обеспечению эффективной работы системы контент-фильтрации;

– практической отработкой способов и порядка использования в образовательном процессе цифровых образовательных ресурсов (ЦОР);

– практической отработкой способов и порядка информационная безопасность локальной сети образовательного учреждения.

Категория слушателей: специалисты органов государственной власти, местного самоуправления, образовательных организаций и учреждений всех видов форм и собственности.

Режим занятий: 36 часов самостоятельной работы в неделю.

В результате изучения курса слушатели должны:

быть ознакомлены:

с нормативными правовыми и организационными основами защиты информации и обеспечения безопасности персональных данных в Российской Федерации;

с порядком применения организационных и технических мер обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду, порядком использования в образовательном процессе цифровых образовательных ресурсов;

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 и технических мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

порядок применения организационных и технических мер обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду;

меры обеспечения безопасности локальной сети образовательной организации;

порядок применения организационных и технических мер обеспечения информационной безопасности детей при использовании ресурсов сети Интернет.

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;

определять состав и содержание мер по обеспечению информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду;

определять состав и содержание мер по обеспечению информационной безопасности детей при использовании ресурсов сети Интернет.

иметь навык:

определения уровня защиты персональных данных;

выявления угроз безопасности персональных данных в информационных системах персональных данных;

применения организационных мер и программно-аппаратных средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных от несанкционированного доступа;

применения организационных мер и программно-аппаратных средств обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду.

применения организационных мер по обеспечению информационной безопасности детей при использовании ресурсов сети Интернет.

ТЕМАТИЧЕСКИЙ ПЛАН ЗАНЯТИЙ

программы повышения квалификации

«Информационная безопасность в образовательной организации»

№ п/п	Название разделов и тем	Всего, часов	в том числе:		
			3	практ. занятия	самост. работа
1	Правовые и организационные вопросы технической защиты информации ограниченного доступа	22	22	-	-
2	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	24	24	-	-
3	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации **в** информационных системах персональных данных	24	24		
4	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	24	24		
5	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	24	24		
6	Основы организации применения организационных мер и программно-аппаратных средств обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду. Использование в образовательном процессе цифровых образовательных ресурсов (ЦОР).	24	24	-	-
Итоговая аттестация - тестирование		2	-	2	-
ИТОГО:		144	142	2	-

1.1. РЕФЕРАТИВНОЕ ОПИСАНИЕ ТЕМ

Раздел № 1. Общие вопросы технической защиты информации

Тема № 1. Правовые и организационные основы технической защиты информации ограниченного доступа

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.

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 № 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты **информации от несанкционированного доступа**

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.

Раздел № 2. Организация обеспечения безопасности персональных данных в информационных **системах персональных данных**

Тема № 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных

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, многоуровневое, персональной ответственности и минимизации привилегий, разделения полномочий и их характеристика. Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Оценка достаточности и обоснованности запланированных мероприятий. Содержание мер защиты информации в информационной системе.

Тема № 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их **обработке в информационных системах 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.

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 № 5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных

Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой 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 персональных данных. Планирование работ по контролю состояния защиты персональных данных в информационных системах персональных данных. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты персональных данных.

Раздел № 3. Анализ государственного регулирования информационной безопасности детства. Защита детей от информации, несовместимой с задачами воспитания и обучения.

Тема № 6. Основы организации применения организационных мер и программно-аппаратных средств обеспечения информационной безопасности образовательных учреждений в контексте

противодействия угрозам терроризма, экстремизма и противодействию суициду. Использование в образовательном процессе цифровых образовательных ресурсов (ЦОР).

Законодательно-правовое регулирование информационной безопасности детей и подростков в Российской Федерации.

Методы и технологии обеспечения информационной безопасности детей и подростков на уровне личности, группы, общества.

Информационная безопасность образовательного учреждения. Использование компьютерных технологий и работа в сети Интернет.

Анализ современных программно-аппаратных средств обеспечения информационной безопасности.

Информационная безопасность образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду. Использование в образовательном процессе цифровых образовательных ресурсов (ЦОР).

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ УЧЕБНОЙ ПРОГРАММЫ

В процессе изучения данной программы необходимо использовать действующие законодательные акты в области защиты персональных данных в информационных системах обработки персональных данных, технической защиты информации, документы национальной системы стандартизации, организационно-распорядительные и нормативные документы ФСТЭК (Гостехкомиссии) России, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите персональных данных в информационных системах обработки персональных данных.

Проводится анализ государственного регулирования информационной безопасности детства. Приводится ряд организационных мер и программно-аппаратных средств обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду.

С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

Теоретические-вопросы по тематике курса, наиболее важные в профессиональной деятельности слушателей, выносятся для обсуждения на семинары. При подготовке к семинарам слушателям заранее выдаются вопросы, подготовка к которым требует самостоятельной работы с использованием рекомендованной литературы.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических занятий по применению программно-аппаратных средств защиты персональных данных при их обработке в информационных системах персональных данных (тема № 2), проводится в компьютерном классе с предварительной установкой необходимого программного обеспечения в компьютерной сети. Для проведения цикла практических занятий выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении практических занятий необходимо отрабатывать задания, учитывающие специфику выполняемых функциональных обязанностей слушателями курсов по своему профессиональному предназначению, в том числе предусматривать задания с проведением деловых игр (эпизодов).

Для проведения практических занятий должны использоваться методические разработки, позволяющие индивидуализировать задания обучаемым в зависимости от их должностных категорий. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями информационных систем персональных данных, и набором конкретных действий, существенных для определённых категорий

обучаемых, объединённых в соответствующую подгруппу.

Самостоятельные занятия проводятся под руководством преподавателя. Для обеспечения занятий используются автоматизированные обучающие системы, электронные учебники, виртуальные автоматизированные системы и компьютерные сети, а также программные средства имитации несанкционированных действий.

В качестве формы итогового контроля полученных знаний выбран зачёт с оценкой, в процессе проведения которого применяются методы тестирования с использованием компьютерных технологий.

Календарный учебный график реализации дополнительной профессиональной программы «Информационная безопасность в образовательной организации» (повышения квалификации)

№ п/п	Наименование дисциплины	Всего ак.часов	Календарные дни													
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
1.	Правовые и организационные вопросы технической защиты информации ограниченного доступа	22	ТЗ-6ч.	ТЗ-6ч.	ТЗ-6ч.	ТЗ-4ч.										
2.	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	24				ТЗ-2ч.	ТЗ-6ч.	ТЗ-6ч.	ТЗ-6ч.	ТЗ-4ч.						
3.	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	24								ТЗ-2ч.	ТЗ-6ч.	ТЗ-6ч.	ТЗ-6ч.	ТЗ-4ч.		
4.	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	14												ТЗ-2ч.	ТЗ-6ч.	ТЗ-6ч.
5.	Практические реализации типовых моделей защищенных информационных систем															

ı	обработки персональных данных															
6.	Основы организации применения организационных мер и программно-аппаратных средств обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду. Использование в образовательном процессе цифровых образовательных ресурсов (ЦОР).															
	Итоговая аттестация															
	Итого	84	6	6	6	6	6	6	6	6	6	6	6	6	6	6

Продолжение

№ п/п	Наименование дисциплины	Всего ак.часов	Календарные дни													
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
1.	Правовые и организационные вопросы технической защиты информации ограниченного доступа															
2.	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные															

'	средства защиты информации от несанкционированного доступа															
3.	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных															
4.	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	10	ТЗ-6ч.	ТЗ-4ч.												
5.	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	24		ТЗ-2ч.	ТЗ-6ч.	ТЗ-6ч.	ТЗ-6ч.	ТЗ-4ч.								
6.	Основы организации применения организационных мер и программно-аппаратных средств обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду. Использование в образовательном процессе цифровых образовательных	24						ТЗ-2ч.	ТЗ-6ч.	ТЗ-6ч.	ТЗ-6ч.	ТЗ-4ч.				

	ресурсов (ЦОР).															
'	Итоговая аттестация	2										ИА-2ч.				
	Итого	60	6	6	6	6	6	6	6	6	6	6				