ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«МК СЕРВИС»

УТВЕРЖДАЮ
Директор
ООО «МК Сервис»

_____М.В. Каверин
«01» февраля 2024 г.

Дополнительная профессиональная программа
повышения квалификации
специалистов по защите информации по направлению
«Информационная безопасность»
«Обеспечение безопасности персональных данных при их обработке
в информационных системах персональных данных»
(72 часа)

г. Тула

1. Общие положения

Программа повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» разработана с учетом требований Федерального закона от 28.12.2010 № 390-ФЗ «О безопасности», Федерального закона от № 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 № 152-ФЗ «О персональных данных», 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», «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Методика оценки угроз безопасности информации».

При разработке программы выполнены требования по разработке дополнительных профессиональных программ, утвержденные приказом Минобразования России от 05.12.2013 № 1310 «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности».

2. Цель обучения

Целью реализации программы является 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.

Объектами профессиональной деятельности обучающихся являются:

– объекты информатизации (ОИ), включающие информационные (автоматизированные) системы различного уровня и назначения, средства и системы обработки информации и средства их обеспечения, а также помещения, предназначенные для ведения переговоров (защищаемые помещения (ЗП));

– технические каналы утечки информации на ОИ и угрозы безопасности информации, реализуемые в отношении автоматизированных рабочих мест (АРМ) и ЗП;

– система нормативно правовых актов, методических документов, национальных и международных стандартов в области технической защиты информации, в том числе персональных данных;

– способы и средства, реализуемые для обеспечения защиты персональных данных.

Поставленная цель достигается решением следующих задач:

– изучение нормативных правовых и организационных основ обеспечения

безопасности персональных данных в информационных системах персональных данных;

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

– анализ практических способов и порядка проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

3. Планируемые результаты обучения

В результате освоения программы слушатель должен приобрести следующие знания и умения: слушатель должен знать:

– содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;

– содержание основных документов национальной системы стандартизации, действующих в области защиты информации;

– 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;

– порядок организации и проведения лицензирования деятельности в области защиты информации;

слушатель должен уметь:

– планировать мероприятия по обеспечению безопасности персональных данных;

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

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

– определять уровень защищенности персональных данных, обрабатываемых в информационных системах персональных данных;

– обосновывать и задавать требования по обеспечению безопасности персональных данных 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 нейтрализации актуальных угроз безопасности персональных данных.

4. Требования к квалификации поступающего на обучение

К освоению программы допускаются:

Лица, имеющие высшее образование по направлению подготовки (специальности) в области информационной безопасности, или прошедшие профессиональную

переподготовку для выполнения нового вида профессиональной деятельности в области информационной безопасности, или имеющие иное высшее образование, подтвержденное документом об образовании, и стаж работы в области защиты информации не менее одного года.

5. Форма обучения

Форма обучения – заочная с применением дистанционных образовательных технологий.

6. Условия реализации программы

Обучение слушателей осуществляется с использованием системы дистанционного обучения (образовательной онлайн площадки).

В рамках Программы повышения квалификации проведение практических занятий осуществляется специалистами высшего уровня квалификации в области защиты персональных данных, имеющими практический опыт работы в российских компаниях и государственных организациях.

Для каждого обучающегося обеспечивается доступ в систему дистанционного обучения, в которой предусмотрены лекции, практические задания, материалы для самопроверки, сервис коммуникаций с преподавателем.

Программа повышения квалификации реализуется в ООО «МК Сервис». Передача Программы другим образовательным организациям не предусматривается.

Изменения и дополнения вносятся в Программу по мере необходимости в целях ее актуализации в случае изменения законодательной базы и осуществляются по распоряжению директора ООО «МК Сервис».

7. Формы аттестации

Аттестация слушателей по итогам прохождения обучения проводится в целях подтверждения усвоения слушателями основного материала, изложенного в процессе обучения.

Аттестация проводится в форме тестирования по всем вопросам, предусмотренным тематическим планом настоящей программы.

Перечень вопросов (тестов), используемых для проведения итоговой аттестации, полностью соответствует и отражает содержание лекционных и практических занятий по всем темам программы.

По результатам аттестации слушателям выдается документ, подтверждающий прохождение обучения.

8. Перечень тем

№ темы	Наименование тем
1.	Раздел № 1. Общие вопросы технической защиты информации
2.	Тема № 1. Правовые и организационные вопросы технической защиты информации ограниченного доступа.

3.	Тема № 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, аппаратные и программные средства защиты информации от несанкционированного доступа.
4.	Раздел № 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных.
5.	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.
6.	Тема № 4. Основы организации и ведения работ по обеспечению безопасности персональных данных
7.	Тема № 5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных.

9. 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 от 02 июля 2021 года. Доктрина информационной безопасности Российской Федерации. Концептуальные основы ТЗИ. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих.

Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации, их задачи, распределение полномочий по обеспечению ТЗИ. Задачи, полномочия и права Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Задачи, полномочия и права управлений ФСТЭК России по федеральным округам.

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

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

Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.

Тема № 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.

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 № 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, 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.

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

УТВЕРЖДАЮ
Директор
ООО «МК Сервис»

_____М.В. Каверин
«01» февраля 2024 г.

Учебный план
Образовательной программы дополнительного профессионального образования
(повышения квалификации)
«Обеспечение безопасности персональных данных при их обработке
в информационных системах персональных данных»

Цель – повышение профессиональных компетенций, необходимых для выполнения обязанностей по должностному назначению в рамках имеющейся квалификации.

Категория слушателей – сотрудники органов власти, организаций и предприятий, осуществляющие эксплуатацию информационных систем, обеспечивающие безопасность информации при ее обработке, хранении и передачи в телекоммуникационных системах и сетях, имеющих высшее или среднее профессиональное образование.

Форма обучения – заочная с применением дистанционных образовательных технологий.

Объем программы – 72 часа.

Режим занятий – по 8 учебных часов ежедневно с перерывами: 10 минут каждые 2 часа, 1 час каждые 4 часа.

№ п/п	Наименование разделов и дисциплин	Часы
1.	**Раздел № 1. Общие вопросы технической защиты информации**	**22**
2.	Тема № 1. Правовые и организационные основы технической защиты информации ограниченного доступа	8
3.	Тема № 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	14
4.	**Раздел № 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных**	**46**
5.	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.	20
6.	Тема №4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	20
7.	Тема №5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных.	6
8.	Итого по видам занятий	68
9.	Экзамен/тест	4
10.	Всего	72