ПРАВИТЕЛЬСТВО МОСКВЫ

ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ

ПИСЬМО
от 22 марта 2010 г. N 2-11-3993

В целях приведения в соответствие с требованиями федерального законодательства работы с персональными данными в системе здравоохранения города Москвы все информационные системы учреждений здравоохранения к 01.01.2011 должны соответствовать требованиям Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" и Федерального закона от 27 декабря 2009 года N 363-ФЗ "О внесении изменений в статьи 19 и 25 Федерального закона "О персональных данных".

Работы, проводимые в учреждениях здравоохранения по организации защиты персональных данных, должны вестись в соответствии с прилагаемым утвержденным Регламентом выполнения мероприятий по организации защиты персональных данных в учреждениях здравоохранения города Москвы.

Первый заместитель руководителя
Департамента здравоохранения
города Москвы
С.В. Поляков

УТВЕРЖДАЮ

Руководитель Департамента
здравоохранения города Москвы
А.П. Сельцовский

РЕГЛАМЕНТ ВЫПОЛНЕНИЯ МЕРОПРИЯТИЙ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УЧРЕЖДЕНИЯХ ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ

1. Введение

В настоящее время в Российской Федерации осуществляется государственное регулирование в области обеспечения безопасности персональных данных. Правовое регулирование вопросов обработки персональных данных проводится в соответствии с Конституцией Российской Федерации и международными договорами Российской Федерации, на основании вступившего в силу с 2007 года Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Федерального закона от 27 декабря 2009 года N 363-ФЗ "О внесении изменений в статьи 19 и 25 Федерального закона "О персональных данных". Во исполнение положений данных Федеральных законов принят ряд федеральных и московских нормативно-правовых актов и методических документов.

В силу требований Федерального закона N 363-ФЗ все информационные системы персональных данных (далее - ИСПДн), созданные до введения его в действие, должны быть приведены в соответствие установленным требованиям не позднее 1 января 2011 года.

Настоящий Регламент определяет последовательность действий для приведения ИСПДн в соответствие с законодательством. Он разработан на основании Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" с учетом действующих нормативных документов ФСТЭК и ФСБ России по защите информации. При его составлении использованы Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости, утвержденные Департаментом информатизации Минздравсоцразвития 23.12.2009.

2. Основные задачи учреждений здравоохранения города Москвы,

эксплуатирующих информационные системы персональных данных

На основании статьи 3 Федерального закона "О персональных данных" учреждения здравоохранения города Москвы являются операторами персональных данных как юридическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание их обработки. В соответствии с законодательством оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Во всех внедряемых информационных системах с момента их ввода в эксплуатацию должна обеспечиваться защита персональных данных. В отношении действующих информационных систем, обрабатывающих персональные данные, учреждения здравоохранения города Москвы, эксплуатирующие системы обязаны решить следующие задачи:

1. Провести классификацию ИСПДн с оформлением соответствующего акта.

2. Реализовать комплекс мер по защите персональных данных в соответствии с перечисленными правовыми актами и методическими документами.

3. Провести оценку соответствия ИСПДн требованиям безопасности в форме сертификации (аттестации) или декларирования соответствия.

Решение поставленных задач достигается совместной работой учреждений здравоохранения, Департамента здравоохранения города Москвы и специализированных организаций с освоением средств, выделяемых на защиту персональных данных. Мероприятия, сроки их выполнения, результаты и ответственные по ним указаны в Плане мероприятий по защите персональных данных в учреждениях здравоохранения города Москвы (приложение к настоящему Регламенту - не приводится). Типовые формы приказов, распоряжений и прочих документов, которые должны быть подготовлены и утверждены учреждением здравоохранения, приведены в приложениях к Методическим рекомендациям для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости, утвержденным Департаментом информатизации Минздравсоцразвития 23.12.2009.

3. Мероприятия по защите персональных данных, самостоятельно проводимые учреждением здравоохранения

Каждое учреждение здравоохранения города Москвы, в котором используется ИСПДн, должно выполнить следующие действия:

1. Начать работу по приведению информационных систем учреждений в соответствие с 152-ФЗ с издания приказа "О защите персональных данных". День выхода приказа считается днем начала работ.

2. В течение трех дней с начала работ должны быть разработаны и изданы в учреждении здравоохранения приказы:

- "О подразделении учреждения, которому поручается защита персональных данных";
- "О назначении лиц, ответственных за обработку персональных данных";
- "О проведении внутренней проверки".

4. Подготовительные мероприятия по защите персональных данных, проводимые учреждением здравоохранения совместно со специализированной организацией

Для выполнения мероприятий по подготовке к созданию системы защиты персональных данных привлекается организация, имеющая необходимые лицензии на проведение работ. Выбор организации осуществляется централизованно, на основании конкурса, проводимого Департаментом здравоохранения, и оформляется Государственным контрактом. Работа организации проводится в соответствии с календарным планом Государственного контракта.

1. После заключения Государственного контракта его исполнитель проводит внутреннюю проверку в учреждении здравоохранения. Результаты проверки должны быть оформлены в виде отчета, который подлежит утверждению руководством учреждения здравоохранения.

2. По результатам проверки исполнителем Государственного контракта разрабатываются документы: "Концепция информационной безопасности учреждения здравоохранения" и "Политика информационной безопасности в учреждении здравоохранения". Документы утверждаются внутри учреждения и вводятся в действие приказом по учреждению здравоохранения.

3. На основании собранных данных в соответствии с утвержденными документами исполнитель Государственного контракта:

- определяет состав и категории обрабатываемых персональных данных. Результат оформляется в виде "Перечня персональных данных, обрабатываемых в учреждении здравоохранения";

- осуществляет классификацию действующих информационных систем, обрабатывающих персональные данные. Результат оформляется в виде "Акта классификации ИСПДн";

- адаптирует модель угроз к конкретной ИСПДн учреждения. Результат оформляется в виде "Модели угроз";

- разрабатывает Положение о разграничении прав доступа к обрабатываемым персональным данным.

4. Как итог выполнения Государственного контракта исполнитель разрабатывает:

- план мероприятий по защите персональных данных;

- техническое задание для организации конкурса на заключение Государственного контракта по проведению технических мероприятий по разработке и созданию системы защиты;

- эскизный проект системы защиты персональных данных в ИСПДн;

- инструкцию администратора ИСПДн;

- инструкцию администратора безопасности;

- инструкцию пользователя при работе с ИСПДн;

- инструкцию пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций.

Используя результаты выполнения Государственного контракта учреждение здравоохранения:

- подготавливает и направляет уведомление в территориальный орган Россвязькомнадзора (уполномоченный орган по защите прав субъектов персональных данных), и тем самым регистрируется в качестве оператора персональных данных;

- назначает ответственных за обеспечение безопасности персональных данных;

- разрабатывает и утверждает внутри учреждения план внутренних проверок состояния защиты персональных данных;

- разрабатывает и утверждает внутри учреждения журнал учета обращений субъектов персональных данных о выполнении их законных прав.

5. Организация надзора за техническими мероприятиями для обеспечения защиты персональных данных, выполняемыми по Государственному контракту

На основании требований технического задания, разработанного при проведении мероприятий по защите персональных данных, самостоятельно проводимых учреждением здравоохранения (раздел 2, п. 6), Государственный заказчик организует конкурс на право заключения Государственного контракта по выполнению соответствующих работ. Победитель конкурса в соответствии с условиями контракта:

1. Разрабатывает и представляет на согласование в учреждение проектную и техническую документацию по системе защиты персональных данных при их обработке в ИСПДн. После согласования учреждением документация утверждается Государственным заказчиком.

2. Поставляет оборудование для системы защиты.

3. Проводит установку и настройку оборудования, осуществляет пусконаладочные работы.

4. Проводит обучение персонала, который будет эксплуатировать систему защиты.

5. Подготавливает эксплуатационную документацию по системе защиты, в том числе проекты документов:

- порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации;

- электронный журнал обращений пользователей информационной системы к ПДн;

- перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним;

- программу и методику аттестационных испытаний.

6. Проводит пробную эксплуатацию и организует предварительные испытания.

7. Подготавливает аттестационные испытания.

Взаимодействуя с исполнителем Государственного контракта, учреждение здравоохранения на этапе проведения технических мероприятий осуществляет общий надзор за работами, а также:

- согласует проектную и техническую документацию по системе защиты персональных данных;

- организует обучение персонала, который будет эксплуатировать систему защиты;

- согласует программу и методику аттестационных испытаний;

- участвует в пробной эксплуатации системы защиты и предварительных испытаниях;

- утверждает документы:

технических средств и программного обеспечения, баз данных и средств защиты информации;

КонсультантПлюс: примечание.
Нумерация подпунктов дана в соответствии с официальным текстом документа.

б) электронный журнал обращений пользователей информационной системы к ПДн;

в) перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним;

г) программу и методику аттестационных испытаний.

6. Проведение аттестационных (сертификационных) испытаний информационных систем персональных данных

После реализации организационно-технических мероприятий по приведению ИСПДн в соответствие с требованиями закона учреждения здравоохранения города Москвы должны провести аттестационные испытания (аттестацию проводит контролирующий орган или специально уполномоченный контролирующим органом лицензиат) или составить декларацию соответствия ИСПДн классу.

Аттестация ИСПДн обязательна для систем К1, К2. Аттестационные испытания проводятся организациями, имеющими необходимые лицензии ФСТЭК России, и состоят из следующих этапов:

а) анализа ИСПДн учреждения, изучения вновь принятых решений по обеспечению безопасности информации и включают проверку:

организационно-технических мероприятий по обеспечению безопасности персональных данных;

защищенности информации от утечек по техническим каналам;

защищенности информации от несанкционируемого доступа;

б) по результатам аттестационных испытаний принимается решение о выдаче "Аттестата соответствия" информационной системы заявленному классу по требованиям безопасности информации. Аттестат выдается сроком на 3 года.

Декларирование соответствия - это подтверждение соответствия характеристик ИСПДн предъявляемым к ним требованиям, установленным законодательством Российской Федерации, руководящими и нормативно-методическими документами ФСТЭК России и ФСБ России. Декларирование соответствия может осуществляться на основе собственных доказательств учреждения или на основании доказательств, полученных с участием привлеченных организаций, имеющих необходимые лицензии.

Для организации проведения аттестации после выполнения технических мероприятий по обеспечению защиты персональных данных (раздел 4) учреждение должно обратиться в Департамент здравоохранения города Москвы.

В случае проведения декларирования на основе собственных доказательств учреждение здравоохранения самостоятельно формирует комплект документов, таких как техническая документация, другие документы и результаты собственных исследований, послужившие мотивированным основанием для подтверждения соответствия информационной системы персональных данных всем необходимым требованиям, предъявляемым к классу К3. Для информационных систем К4 оценка соответствия не регламентируется и осуществляется по решению учреждения.

7. Прием в промышленную эксплуатацию и организация эксплуатации системы защиты персональных данных при их обработке в ИСПДн

Прошедшая аттестацию система защиты персональных данных при их обработке в ИСПДн должна быть принята в промышленную эксплуатацию в качестве отдельной системы или как подсистема ИСПДн. Для этого в соответствии с Московским законодательством должно быть издано распоряжение Правительства Москвы.

Учреждение здравоохранения:

готовит проект распоряжения Правительства Москвы о приеме системы в промышленную эксплуатацию.

После выхода распоряжения обеспечивает занесение данных о системе в Реестр информационных ресурсов и систем города Москвы.

Организует сопровождение работы системы (подсистемы) защиты персональных данных ИСПДн.

8. Принятые сокращения

ИСПДн - информационные системы персональных данных.