Администрация Выборгского района г. Санкт-Петербурга

СПб ГБУЗ «ДЕТСКАЯ ГОРОДСКАЯ ПОЛИКЛИНИКА № 17»

УТВЕРЖДАЮ

Главный врач
СПб ГБУЗ «Детская городская
поликлиника № 17»
А.Н. Игошина

(подпись)
«01» 07 2022 г

М.П.

Положение по защите персональных данных
СПб ГБУЗ «Детская городская поликлиника № 17»

г. Санкт-Петербург

2022

Общие положения

Положение по защите персональных данных (далее - положение) регламентирует организацию и проведение работ по защите персональных данных, обрабатываемых в ИСПДн Санкт- Петербургского государственного бюджетного учреждения здравоохранения «Детская городская поликлиника М 17» (далее - Учреждения).

Основание для разработки

Настоящее Положение разработано в соответствии со следующими нормативно-правовыми документами:

- Статья 24 Конституции Российской Федерации;

- Глава 14 «Защита персональных данных работника» Трудового Кодекса Российской Федерации;

- Федеральный закон Российской Федерации № 152-ФЗ «О персональных данных» от 27 июля 2006 г.

- Федеральный закон Российской Федерации № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. (в ред. От 30.12.2021г.);

- Постановление Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г.;

- Постановление Правительства Российской Федерации № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г.;

Приказ ФСТЭК г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. (в ред. От 14.05.2020г.);

Область действия

Положения настоящего документа обязательны для исполнения работниками Учреждения, допущенными к обработке персональных данных.

Действие настоящего документа распространяется на все информационные системы персональных данных (ИСПДн) Учреждения.

Порядок ввода в действие и внесения изменений в настоящее Положение утверждается главным врачом Учреждения и вводится его приказом. Все изменения вносятся приказом главного врача Учреждения.

Все сотрудники Учреждения, осуществляющие обработку персональных данных, должны быть ознакомлены под расписку с данным Положением и изменениями к нему.

2 Организация работ па обеспечению безопасности ПДн

Основные положения

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятии, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн. Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой Системы защиты персональных данных (далее - СЗПДн).

Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки, а также используемые в информационной системе информационные технологии).

Состав, категории и местонахождение ПДн определяют замысел защиты при обработке ПДн в ИСПДн Учреждения.

Организация защиты ПДн подразумевает проведение мероприятий, направленных на недопущение несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Порядок организации обеспечения безопасности ПДн в ИСПДн предусматривает:

- оценку текущего состояния обеспечения безопасности ПДн;
- обоснование требований по обеспечению безопасности Идн на основании определенного класса ИСПДн и формулирование задач защиты ПДн;
- выбор целесообразных способов (мер и средств) защиты ПДн;
- организацию и проведение работ по созданию системы защиты персональных данных (СЗПДн) в рамках разработки (модернизации) ИСПДн, решение основных

задач взаимодействия, определение задач и функций на различных стадиях созданиях и эксплуатации СЗПДн;

-разработку документов, регламентирующих вопросы организации защиты ПДн и эксплуатации СЗПДн в ИСПДн;

- развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн;
- доработку СЗПДн по результатам опытной эксплуатации.

Оценка текущего состояния безопасности ПДн

Оценка текущего состояния обеспечения безопасности ПДн основывается на результатах внутренней проверки.

При оценке текущего состояния обеспечения безопасности ПДн определяется необходимость обеспечения безопасности ПДн от угроз безопасности персональных данных.

При оценке текущего состояния обеспечения безопасности ПДн учитывается степень ущерба, который может быть причинен в случае неправомерного использования соответствующих ПДн, а также проводится анализ имеющихся в распоряжении мер и средств защиты ПДн.

Обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн

Обоснование требований по обеспечению безопасности ПДн, обрабатываемых в ИСПДн, проводится в соответствии с нормативными и методическими документами уполномоченных федеральных органов исполнительной власти, обязательными к применению стандартами . При этом выявление и оценка актуальности угроз безопасности персональных данных при их обработке в ИСПДн осуществляется в соответствии с методическими документами ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14 февраля 2008 г. и «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 г.

СЗПДн ИСПДн Учреждения предназначена для решения следующих задач по защите:

- идентификация пользователя в ИСПДн;
- проверка прав доступа к защищаемым данным в рамках общезначимого (системного) контекста безопасности;
- обеспечение целостности данных в ИСПДн;
- предотвращение попыток получения НСД к ПДн, обрабатываемых в ИСПДн Учреждения;

- предотвращение несанкционированного, в том числе случайного, уничтожения, изменения, блокирования, копирования, распространения персональных данных.

Способы и меры защиты ПДн

По способам защиты все меры обеспечения безопасности ПДн при их обработке в ИСПДн подразделяются на правовые, организационные и технические.

К правовым мерам относится регламентация законами и нормативными актами действий с информацией и оборудованием, и наступление ответственности за нарушение требований указанных законов и актов.

К организационным мерам относятся меры, регламентирующие процессы функционирования ИСПДн, порядок использования их ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы максимально снизить возможность реализации угроз безопасности ПДн.

Организационные меры включают:

- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);

- организацию охраны и режима допуска к элементам ИСПДн;

- организацию учета, хранения, использования и уничтожения документов и носителей информации, содержащей ПДн.

Определение перечня персональных данных, обрабатываемых в Учреждении. Определение цели обработки персональных данных. Затем нужно определить цели обработки персональных данных: трудовые отношения с работниками; оформление пропусков для входа на территорию предприятия; договор оказания услуг и т.п.

Определение сроков обработки и хранения ПДн. Хранение ПДн должно быть не дольше, чем этого требуют цели их обработки, по достижению которых Йдн подлежат уничтожению. Установить перечень ПДн, по которым цели обработки достигнуты.

Определение ответственных за обеспечение безопасности ПДн. Определение круга лиц, допущенных к обработке персональных данных.

Обучение сотрудников. Не реже одного раза в год необходимо проводить обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними.

Также проводится обучение сотрудников Учреждения, допущенных к обработке ПДн, правилам обработки ПДн, в соответствии с утвержденными требованиями.

Установление персональной ответственности за нарушения правил обработки ПДн. В должностные инструкции сотрудников, допущенных к обработке ПДн, должны быть внесены изменения в части персональной ответственности за нарушение правил обработки ПДн.

Учет применяемых технических средств защиты персональных данных.

Учет носителей персональных данных. В обязательном порядке должен проводиться учет всех защищаемых носителей персональных данных.

Разработка организационно - распорядительных документов (далее ОРД).

Необходимо разработать пакет ОРД, которые будут регламентировать весь процесс получения, обработки, хранения, передачи и защиты персональных данных.

Технические меры защиты ПДн предполагают использование программно -аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов Учреждения.

Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

Организация и проведение работ по созданию системы защиты персональных данных

Создание СЗПДн является необходимым условием обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиями к обеспечению безопасности ПДн для ИСПДн соответствующего класса и/или не покрывают всех угроз безопасности или для данной ИСПДн.

Рекомендуются следующие стадии создания СЗПДн:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на создание СЗПДн;

- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн; стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также о соответствия ИСПДн требованиям безопасности информации.

На предпроектной стадии по обследованию ИСПДн выполняются следующие мероприятия:

- Устанавливается необходимость обработки ПДн в ИСПДн.
- Определяется перечень ПДн, подлежащих защите.

- Определяются условия расположения ИСПДн относительно границ контролируемой зоны.

- Определяются конфигурация и топология ИСПДн в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения.

- Определяются технические средства и системы, предполагаемые к использованию в разрабатываемой ИСПДн, условия их расположения, обще системные и прикладные программные средства, имеющиеся и предлагаемые к разработке.

- Определяются режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах.

- Уточняется степень участия персонала в обработке ПДн, характер их взаимодействия между собой.

- Определяются (уточняются) угрозы безопасности ПДн к конкретным условиям функционирования (разработка Частной модели угроз ПДн).

- Определяется класс ИСПДн. Классификация ИСПДн проводится в соответствии с порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

На стадии проектирования и создания СЗПДн проводятся следующие мероприятия:

- Разработка задания и проекта на создание (реконструкцию) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн.

- Разработка раздела технического проекта на ИСПДн в части защиты информации.

- Разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями.

- Использование сертифицированных технических, программных и программно-технических средств защиты информации и их установка.

- Сертификация по требованиям безопасности информации программных средств защиты информации, в случае, когда на рынке отсутствуют требуемые сертифицированные средства защиты информации.

- Разработка и реализация разрешительной системы доступа пользователей к обрабатываемой на ИСПДн информации.

- Определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением по направлению обеспечения безопасности ПДн.

На стадии ввода в действие СЗПДн осуществляются:

- Генерация пакетов прикладных программ в комплексе с программными средствами защиты информации.

- Опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн и отработки ПДн.

- Приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

- Оценка соответствия ИСПДн требованиям безопасности ПДн.

Оценка соответствия ИСПДн по требованиям безопасности ПДн проводится:

- для ИСПДн 1 и 2 классов - обязательная сертификация (аттестация по требованиям безопасности информации);

- для ИСПДн 3 класса - декларирование соответствия требованиям безопасности информации (оформляется документ «декларация соответствия ИСПДн, требованиям по обеспечению безопасности ПДн»);

- для ИСПдн 4 класса оценка соответствия проводится по решению руководства Организации.

3 Обязанности должностных лиц в части обеспечения безопасности защиты персональных данных

Администратор ИСПДн обязан осуществлять контроль над соблюдением установленного регламентирующими документами режима при обработке персональных данных, пресекать действия сотрудников и других лиц, которые могут привести к утечке или разрушению защищаемой информации, и сообщать о фактах таких действий ответственному за обеспечение защиты персональных данных.

- Пользователи ПЭВМ, занятые обработкой персональных данных обязаны знать и соблюдать требования по безопасности персональных данных, в части, их касающейся;

- строго следить за соблюдением режима разграничения доступа, незамедлительно информировать администратора безопасности о всех случаях утечки или разрушения обрабатываемой на ПЭВМ защищаемой информации;

- соблюдать правила обращения с документами, содержащими персональные данные, порядок их получения, обработки и хранения;

- строго соблюдать установленные в Учреждении правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

- во время работы с документами, содержащими ПДн, исключать возможность ознакомления с ними иных лиц, не имеющих доступа к данным документам Сотрудникам, которые обрабатывают персональные данные, запрещается:

- разглашать лицам, не имеющим допуска к работе с защищаемой информацией, сведения о технологическом процессе обработки этой информации;

- сообщать устно или письменно свой персональный пароль другим лицам, в том числе допущенным к работе на ПЭВМ;

- набирать на клавиатуре при посторонних лицах свой персональный пароль и записывать его;

- работать с отображенной на экране ПЭВМ защищаемой информацией в присутствии лиц, не имеющих допуска к работе с защищаемой информацией;

- оставлять электронные носители с защищаемой информацией без контроля;

- оставлять без контроля включенную ПЭВМ после выполнения процедуры аутентификации пользователя;

- самостоятельно отключать соединительные кабели, производить какие-либо ремонтные работы;

- снимать защитные крышки корпуса системного блока и другого оборудования, перемещать технические устройства после их включения, подключать бытовые приборы к сети гарантированного электропитания;

- выносить документы и другие носители, содержащие персональные данные, за пределы территории Учреждения без разрешения руководителя структурного подразделения;

- знакомить работников других структурных подразделений, не имеющих доступа к персональным данным субъектов ПДн по своим функциональным обязанностям, с документами, содержащими персональные данные, без письменного разрешения (резолюции) руководителя структурного подразделения, а представителей иных организаций - без наличия письменного согласия субъекта Идн (за исключением случаев, когда передача персональных данных субъекта без его согласия допускается действующим законодательством РФ);

- передавать информацию, содержащую персональные данные, по каналам телефонной и факсимильной связи, с использованием сети Интернет, если меры по защите информации не приняты;

- использовать чужое имя пользователя и пароль для доступа к ресурсам ИСПДн.

Разглашение персональных данных субъектов ПДн (передача их посторонним лицам, в том числе работникам Учреждения, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативными актами (приказами, распоряжениями) Учреждения, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарного взыскания, если иное не предусмотрено законодательством РФ.

Работник Учреждения, имеющий доступ к персональным данным субъектов и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Учреждению (п.7 ст.243 Трудового кодекса РФ).

Ответственность за организацию защиты ПДн возлагается на главного врача Учреждения.

4 Порядок доступа сотрудников к ПДн

Доступ к персональным данным субъектов ПДн имеют работники Учреждения, которым персональные данные субъектов необходимы в связи с исполнением ими трудовых обязанностей. Перечень работников, имеющих доступ к персональным данным, определен в Положении о разграничении прав доступа к персональным данным.

В случае, если Учреждению оказывают услуги юридические и физические лица на основании заключенных договоров, в силу которых им может быть предоставлен доступ к конфиденциальной информации (в т.ч. к персональным данным субъектов), то до начала работ должно быть подписано соглашение о неразглашении конфиденциальной информации между Учреждением и указанными физическими или юридическими лицами.

Процедура оформления допуска к персональным данным включает в себя:

- принятие на себя обязательств перед Учреждением по нераспространению сведений, составляющих конфиденциальную информацию (отражаются в трудовом договоре);
- принятие решения руководителем Учреждения о допуске оформляемого лица к ПДн.
- ознакомление допущенного работника под роспись с нормативными актами (приказы, распоряжения, инструкции и т.п.), регулирующими обработку и защиту ПДн.

Доступ к персональным данным субъектов других работников Учреждения, не имеющих надлежащим образом оформленного допуска, запрещается.

5 Контроль состояния работ по обеспечению безопасности ПДн

Контроль состояния защиты ПДн осуществляется с целью своевременного выявления и предотвращения утечки информации, содержащей ПДн, по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на ПДн.

Задачи контроля:

- своевременное обнаружение и устранение неисправностей, которые могут повлечь утечку информации, содержащей ПДн;
- обучение и информирование лиц, осуществляющих обработку ПДн,
- анализ и составление заключений по фактам нарушений, приводящих к снижению уровня защищенности персональных данных,

- разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений

- обеспечить оперативное обнаружение случаев несанкционированной, неправомерной передачи персональных данных.

Внутренние проверки проводятся в подразделениях Учреждения, участвующих в обработке ПДн, не реже 2-х раз в год.

Внутренние проверки проводятся для:

- обеспечения соответствия требованиям настоящего Положения, а также других нормативных документов по защите ПДн (внутренних документов Учреждения, законодательных актов);

- подтверждения эффективного внедрения и поддержания в состоянии работоспособности СЗПДн.

Организацию и проведение внутренних проверок осуществляет ответственный за обеспечение защиты персональных данных при использовании ПЭВМ.

При проведении проверки должен присутствовать руководитель проверяемого подразделения.

Заключение о состоянии защиты ПДн по результатам проверки и выявленные несоответствия заносятся проверяющим в Отчет по результатам проверки, который согласовывается с руководством Учреждения.

В случае выявления несоответствий организуется расследование причин нарушения. Расследование нарушений осуществляется комиссией, в состав которой входят ответственный за обеспечение защиты персональных данных по учреждению, ответственный за обеспечение защиты персональных данных при использовании ПЭВМ, начальник подразделения, в котором произошло нарушение. При необходимости в качестве экспертов могут привлекаться работники других подразделений Учреждения.

Результаты работы комиссии оформляются в виде заключения с рекомендациями, которое утверждается руководителем Учреждения, после чего принимаются меры по недопущению повторения подобных нарушений.