УТВЕРЖДАЮ
Главный врач ГАУЗ «Детская городская поликлиника №4»
_____ Н.Э.Галеев
_____ 2013г.

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных пациентов при их обработке в информационных системах персональных данных ГАУЗ «Детская городская поликлиника №4»

Настоящее Положение разработано в соответствии с Федеральным Законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», нормативными документами ФСТЭК и ФСБ России с целью обеспечения защиты прав и свобод граждан при обработке их персональных данных в информационных системах персональных данных.

Для целей настоящего Положения применяются следующие термины и определения:

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, состояние здоровья, другая информация.

Оператор Персональных данных - Государственное автономное учреждение здравоохранения «Детская городская поликлиника №4» (далее Учреждение) - субъект, организующий и осуществляющий обработку персональных данных, а также определяющий цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Пользователь информационной системы персональных данных -лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа к информационным системам персональных данных - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Обработка персональных данных - действия (операции) с персональными данными, включающие сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных "данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных - 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 таковых.

Конфиденциальность персональных данных - обязательное для соблюдения работодателем - оператором или иным получившим доступ к персональным данным лицом, требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия) к информационным системам персональных данных - доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

Защита информации - комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным, при этом предусматривается:

- разграничение полномочий доступа к данным;
- авторизация, контроль и учет действий с данными (регистрация событий);
- контроль копирования, печати, обмена данными по каналам связи;
- межсетевое экранирование и защита от вирусов;
- учет внешних носителей данных;
- резервное копирование / восстановление данных;
- раздельное хранение носителей данных с резервными копиями;
- контроль доступа в помещения и к компьютерам;
- применение устройств идентификации пользователей для доступа.

1 Общие положения

Настоящим Положением определяется структура и составляющие безопасности информации в информационной системе персональных данных работников Учреждения и граждан.

Обеспечение безопасности персональных данных (ПДн) при их обработке в автоматизированных системах (информационных системах персональных данных — ИСПДн) достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Мероприятия по обеспечению безопасности ПДн формулируются в зависимости от класса ИСПДн с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, Общества и Государства.

При обеспечении безопасности ПДн проводятся мероприятия, направленные на:

- предотвращение несанкционированного доступа (НСД) к ПДн и (или) передачи их лицам, организациям, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов НСД к ПДн;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- оперативное резервирование информации в ИСПДн;
- реализацию возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;
- постоянный контроль над обеспечением уровня защищенности ПДн.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных (СЗПДн), в соответствии с утвержденными Требованиями по обеспечению безопасности персональных данных

при их обработке в информационных системах персональных данных Учреждения (Приложение № 1).

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 ПДн), а также используемые в информационной системе информационные технологии.

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн; на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз. Обеспечение безопасности ПДн при их обработке в автоматизированных ИСПДн должно проводиться путем выполнения комплекса организационных и технических мероприятий (применения технических средств), в рамках системы (подсистемы) защиты персональных данных, развертываемой в ИСПДн в процессе ее создания или модернизации.

Порядок организации обеспечения безопасности ПДн в ИСПДн предусматривает:

- оценку обстановки;
- обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;
- разработку замысла обеспечения безопасности ПДн;
- выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и замыслом защиты;
- решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;
- обеспечение реализации принятого замысла защиты;
- планирование мероприятий по защите ПДн;
- организацию и проведение работ по созданию СЗПДн в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДн или ее элементов в ИСПДн, решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн;
- разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн.

Мероприятия по обеспечению безопасности персональных данных при их обработке в.ИСПДн включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию разрешенных лицензионных средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с ПДн в информационной системе;

з) контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

Технические и программные средства должны удовлетворять устанавливаемым в соответствий с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности ПДн при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

По структуре ИСПДн, на которые направлена реализация мероприятий по защите, выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автоматизированного рабочего места;
- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем;
- угрозы, реализуемые в ИСПДн при их подключении к сетям связи общего пользования.

Для обеспечения безопасности ПДн при их обработке в информационных системах проводятся:

- обследование и оформление документа о классе информационной системы Учреждения, определение способов и состава средств защиты информации (СЗИ), разработка технического задания (ТЗ) на создание комплексной

системы защиты информации, в том числе разработка модели угроз, проектирование;

- ввод в эксплуатацию - закупка и инсталляция сертифицированных СЗИ, обучение персонала, издание приказов о допуске персонала и регламентов обработки конфиденциальной информации.

2 Цели обеспечения информационной безопасности

2.1 Стратегической целью обеспечения безопасности информации в ИСПДн является защита интересов субъектов информационных отношений. Данная цель достигается посредством постоянного поддержания следующих свойств информации в процессе ее обработки, хранения и передачи:

- целостности информации;
- доступности обрабатываемой информации для зарегистрированных пользователей;
- конфиденциальности информации.

3 Объект защиты

Объектом защиты является информационная система персональных данных работников Учреждения и граждан:

а) Информационные ресурсы:

- персональные данные работников и граждан (исходная информация, информационные базы данных);
- инструментальная информация (программное обеспечение), с помощью которой обрабатывается, хранится и передается информация ПДн;

б) технические информационные системы и средства Учреждения, в которых обрабатывается, хранится и передается информация ПДн;

в) помещения объектов Учреждения, в которых размещаются информационные ресурсы, и обрабатывается конфиденциальная информация;

г) технические системы жизнеобеспечения, электропитания, проводного вещания, охранной сигнализации, обеспечивающие или размещаемые совместно с оборудованием ИСПДн.

Критичными свойствами объекта защиты являются:

а) возможность разрушения или повреждения информационных систем персональных данных в результате пожара, затопления, аварии инженерных систем жизнеобеспечения;

б) возможность прекращения или нарушения нормального функционирования ИСПДн в результате повреждения отдельных их элементов;

в) несанкционированная доступность информации, выражающаяся в возможности:

- непосредственного доступа к информации, находящейся на первичном или вторичном носителе, в транспортной среде передачи; воздействия на

носитель или транспортную среду с целью перлюстрации, отчуждения, копирования, изменения, подмены и уничтожения информации;
- прямого или косвенного доступа к оборудованию ИСПДн и транспортной среде передачи с целью получения доступа к информации (несанкционированный доступ);
- перехвата речевой информации по акустическим и другим каналам утечки (подслушивание).

4Субъекты информационных отношений

4.1 Субъектами информационных отношений являются:
- работники;
- граждане;

4.2 Перечисленные субъекты информационных отношений заинтересованы в обеспечении:
- конфиденциальности (сохранения в тайне) информации в соответствии с требованиями российского законодательства;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);
- своевременного доступа (за приемлемое для них время) к необходимой им информации;
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты информации от незаконного ее тиражирования (защиты персональных данных, защиты авторских прав, прав собственника информации).

5 Возможные угрозы и участки вторжения

Общая классификация угроз.

1. Угрозы конфиденциальности данных и программ. Реализуются при несанкционированном доступе к программам, данным, каналам связи, при перехвате электромагнитных излучений, при анализе трафика.
2. Угрозы целостности данных, программ, аппаратуры. Реализуются при несанкционированном уничтожении, модификации данных, порождении фальсифицированных данных, задержке и нарушении маршрутизации данных в каналах связи.

3. Угрозы доступности данных. Реализуются при создании условий, когда законный пользователь или процесс не получает своевременного доступа к данным или ресурсам системы, каналам связи.

4. Угрозы отказа от выполнения транзакций. Реализуются при создании условий легальному пользователю для отказа от выполненной операции по передаче или приему информации.

6 Порядок проведения контрольных мероприятий и действий по результатам контроля

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Контроль . может проводиться Комиссией, созданной в Учреждении, или на договорной основе сторонними организациями, при наличии лицензии на деятельность по технической защите конфиденциальной информации.

Решение основных вопросов обеспечения защиты ПДн предусматривает подготовку кадров, выделение необходимых финансовых и материальных средств, закупку программного и аппаратного обеспечения.