

**ПОЛОЖЕНИЕ**  
**О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ЗАЩИТЕ**  
**КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (ПЕРСОНАЛЬНЫХ**  
**ДАННЫХ) В ГОБУЗ «ОБЛАСТНАЯ ДЕТСКАЯ КЛИНИЧЕСКАЯ**  
**БОЛЬНИЦА»**

## **1. Термины и определения**

1.1. 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, другая информация.

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

1.3. Информационная система персональных данных (далее - ИСПДн) - 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 таких средств.

1.4. Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.5. Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных.

1.6. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

1.7. Уполномоченное оператором лицо – лицо, которому на основании договора оператор поручает обработку персональных данных.

## **2. Общие положения**

2.1. Настоящее положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в ИСПДн, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием и без использования средств автоматизации, в ГОБУЗ «Областная детская клиническая больница».

2.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

2.3. Обработка персональных данных в ГОБУЗ «Областная детская клиническая больница» осуществляется на основе принципов:

- законности целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

## **3. Порядок определения защищаемой информации**

3.1. Структурные подразделения ГОБУЗ «Областная детская клиническая больница»

создают в пределах своих полномочий ИСПДн, в целях обеспечения реализации прав объектов персональных данных.

3.2. В ГОБУЗ «Областная детская клиническая больница» на основании «Перечня сведений конфиденциального характера», утвержденного Указом Президента Российской Федерации 6 марта 1997 года № 188, определяется и утверждается перечень информационных систем персональных данных. Определяется и утверждается список структурных подразделений ГОБУЗ «Областная детская клиническая больница», в которых осуществляется обработка персональных данных.

3.3. На стадии проектирования каждой ИСПДн определяются цели и содержание обработки персональных данных, утверждается перечень обрабатываемых персональных данных.

#### **4. Основные условия проведения обработки персональных данных**

4.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, составленного по форме согласно приложению 1 к настоящему Положению или сформированного в информационной системе персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Новгородской области за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

4.2. Оператором ИСПДн структурных подразделений ГОБУЗ «Областная детская клиническая больница», организующим и осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных является ГОБУЗ «Областная детская клиническая больница». Обязанности оператора в установленном порядке возлагаются на структурные подразделения ГОБУЗ «Областная детская клиническая больница», осуществляющие деятельность по эксплуатации ИСПДн.

4.3. 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.

4.4. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в ИСПДн оператором назначается должностное лицо, ответственное за обеспечение безопасности персональных данных. Данные должностные лица взаимодействуют по вопросам организации защиты персональных данных в ИСПДн со специалистами ГУЗ МИАЦ.

4.5. Руководители структурных подразделений ГОБУЗ «Областная детская клиническая больница», в чьем ведении находится ИСПДн, определяют служащих, допущенных к обработке персональных данных, и представляют списки данных лиц в управление информатизации и автоматизации.

4.6. Служащие, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации, содержащей персональные данные, по форме согласно приложению 2 к настоящему Положению. Должностные инструкции служащих, допущенных к обработке персональных данных, должны содержать сведения о допуске к персональным данным и основания, на котором данный допуск осуществлен.

4.7. Оператором и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных. Оператор или иное получившее доступ к персональным данным лицо обязано не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

4.8. В случае, если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

## **5. Правила обработки и защиты персональных данных в информационных системах с использованием и без использования средств автоматизации**

5.1. Обработка персональных данных в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями «Положения об обеспечении

безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства Российской Федерации от 17.11.2007 № 781, нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

5.2. Обработка персональных данных без использования средств автоматизации (в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации) осуществляется в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства Российской Федерации 15.09.2008 № 687.

5.3. Оператором осуществляется классификация информационных систем персональных данных в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" в зависимости от категории обрабатываемых данных и их количества.

5.4. Мероприятия по обеспечению безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с «Положением о методах и способах защиты информации в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 5 февраля 2010 года №58.

5.5. На стадии ввода в эксплуатацию ИСПДн проводится ее оценка соответствия требованиям безопасности информации (аттестация по требованиям безопасности информации).

5.6. Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации ИСПДн, инструкции пользователя, администратора безопасности, и других нормативных и методических документов;

- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и

технических средств в соответствии с требованиями безопасности информации;

- охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

## **6. Требования к обработке и защите персональных данных в информационных системах без использования средств автоматизации**

6.1 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных были:

- определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

- обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

6.2. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

- а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

- б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.3. При использовании внешних электронных носителей информации с персональными данными, к ним предъявляются следующие требования:

а) электронные носители информации, содержащие персональные данные, учитываются в журнале учета, выдачи и уничтожения машинных носителей данных, предназначенных для обработки и хранения информации ограниченного доступа, не относящейся к государственной тайне, персональных данных, в ГОБУЗ «Областная детская клиническая больница»;

б) к каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

6.4. Все документы, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы условия, обеспечивающие их сохранность.

## **7. Порядок привлечения специализированных сторонних организаций к разработке ИСПДн и средств защиты информации ГОБУЗ «Областная детская клиническая больница»**

7.1. Порядок привлечения специализированных сторонних организаций к разработке и эксплуатации новых ИСПДн, их задачи и функции на различных стадиях создания и эксплуатации ИСПДн определяются руководителем ГУЗ «МИАЦ», исходя из особенностей автоматизированных систем и по согласованию с управлением информатизации и автоматизации ГОБУЗ «Областная детская клиническая больница» и специалистом по технической защите информации.

7.2. Разработка систем защиты персональных данных в ИСПДн ГОБУЗ «Областная детская клиническая больница», контроль за эксплуатацией ИСПДн осуществляется

ответственным за обеспечение безопасности персональных данных совместно со специалистами ГУЗ «МИАЦ». При необходимости привлекаются специалисты по защите информации подведомственных организаций и специализированных сторонних организаций.

7.3. Для проведения мероприятий по обеспечению безопасности персональных данных для ИСПДн специализированные сторонние организации должны иметь лицензии ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

## **8. Ответственность должностных лиц**

Сотрудники ГОБУЗ «Областная детская клиническая больница», допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

**Приложение 1**  
к положению о порядке организации и  
проведению работ по защите  
конфиденциальной информации  
(персональных данных)

**СОГЛАСИЕ**

**НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Я, \_\_\_\_\_,  
(Ф.И.О.)  
проживающий по адресу: \_\_\_\_\_

Паспорт № \_\_\_\_\_, выданный (кем и когда) \_\_\_\_\_

настоящим даю свое согласие на обработку в ГОБУЗ «Областная детская клиническая больница», 173020, г. Великий Новгород, ул. Державина, д. 1 (далее оператор) моих персональных данных.

Я даю согласие на использование моих персональных данных в целях \_\_\_\_\_.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу третьим лицам), обезличивание, блокирование, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными, предусмотренных действующим законодательством Российской Федерации.

Оператор гарантирует, что обработка моих личных данных осуществляется в соответствии с действующим законодательством Российской Федерации.

Я проинформирован, что оператор будет обрабатывать мои персональные данные как неавтоматизированным, так и автоматизированным способом обработки.

Данное Согласие действует до достижения целей обработки моих персональных данных, установленных действующим законодательством Российской Федерации.

Согласие может быть отозвано по моему письменному заявлению.

Я подтверждаю, что, давая такое Согласие, я действую своей волей и в своих интересах.

Дата: \_\_\_\_\_ Подпись \_\_\_\_\_

**Приложение 2**  
к положению о порядке организации и  
проведению работ по защите  
конфиденциальной информации  
(персональных данных)

**ОБЯЗАТЕЛЬСТВО**

**о неразглашении информации, содержащей персональные данные**

Я, \_\_\_\_\_, (Ф.И.О.)

исполняющий (ая) должностные обязанности по замещаемой должности

\_\_\_\_\_  
(должность, наименование структурного подразделения)

предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному руководителю.
3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.
4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.
5. После прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к ответственности в соответствии с законодательством Российской Федерации.

\_\_\_\_\_

(фамилия, инициалы)

\_\_\_\_\_

(подпись)

« \_\_\_ » \_\_\_\_\_ г.