|  |  |
| --- | --- |
| **УТВЕРЖДАЮ**Главный врач ОГБУЗ «ИГПЦ»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_О.В. Бортник  | Приложение №\_\_\_ к приказу № \_\_\_\_От «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |

**ПОЛОЖЕНИЕ**

об обработке и защите персональных данных работников ОГБУЗ «Иркутский городской перинатальный центр»

|  |  |
| --- | --- |
|  | **СОГЛАСОВАНО**: |
|  |

|  |  |
| --- | --- |
| Начальник отдела кадров *Маркеева О.А.* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Юрисконсульт*Меньшиков А.В.* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Главный специалист по защите персональных данных*Калиниченко Д.В.* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Главный бухгалтер *Бочкарева О.Т.* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Заместитель главного врача по финансово-экономической работе*Гудыно Т.Ю.* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

 |

г. Иркутск

20\_\_\_ г.

# ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
	1. Настоящим Положением об обработке и защите персональных данных Работников (далее – Положение) устанавливается порядок обработки персональных данных Работников ОГБУЗ «Иркутский городской перинатальный центр» (далее Центр или Работодатель) и гарантии конфиденциальности сведений, предоставляемых Работником Работодателю.
	2. Работниками являются физические лица (субъекты персональных данных), заключившие с Работодателем трудовые договоры.
	3. Обработка персональных данных Работников в Центре заключается в сборе, записи, систематизации, накоплении, хранении, уточнении (обновлении, изменении), извлечении, использовании, передаче (распространении, предоставлении, доступе), обезличивании, блокировании, удалении, уничтожении и в защите от несанкционированного доступа к персональным данным.
	4. Настоящее Положение и изменения к нему утверждаются Главным врачом Центра и вводятся в действие приказом по основной деятельности Центра. Все Работники Центра должны быть ознакомлены под подпись с данным Положением и изменениями к нему.
	5. Настоящее Положение является обязательным для исполнения всеми Работниками Центра, имеющими доступ к персональным данным Работников.
	6. Положение утверждается Главным врачом Центра. Документ должен быть согласован с заинтересованными должностными лицами, работниками бухгалтерии, юридической службой, отделом кадров, с финансово-экономическим блоком. Сотрудники, принимаемые на работу, знакомятся с Положением точно так же, как и с другими локальными нормативно-распорядительными актами организации, правилами внутреннего трудового распорядка, положением об оплате труда, должностной инструкцией и др. При этом в соответствии со ст. 68 ТК РФ такое ознакомление Работодатель обязан проводить под роспись до подписания трудового договора.
2. **ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ**
	1. Под персональными данными Работников понимается информация, необходимая Работодателю в связи с трудовыми отношениями и касающаяся конкретного Работника, а также сведения о фактах, событиях и обстоятельствах жизни Работника, позволяющие идентифицировать его личность.
	2. Персональные данные Работника, обработка которых осуществляется в Центре, включают следующие документы и сведения:
* фамилия, имя, отчество;
* фамилия при рождении (либо другие фамилии, если они были);
* день, месяц, год и место рождения;
* паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ);
* гражданство;
* адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;
* номера телефонов (мобильного и домашнего), в случае их регистрации на субъект персональных данных или по адресу его места жительства;
* сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения);
* копии документов об образовании;
* сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и иные сведения;
* копии документов о повышении квалификации;
* сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса и телефона работодателя, а также реквизитов иных организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, а также иные сведения;
* данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и дата изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
* вторые экземпляры трудового договора с Работниками;
* сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
* трудовые книжки и вкладыши к ним;
* карточки унифицированной формы Т-2 «Личная карточка работника»;
* личные дела Работников в бумажной форме;
* фотографическое изображение работника;
* сведения о заработной плате (номера счетов для расчета с Работниками, в том числе номера их банковских карточек);
* сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии\снятии на(с) учет(а) и иные сведения;
* копии военных билетов;
* сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и) или иных членов семьи, паспортные данные супруга(и) или иных членов семьи (паспортные данные или данные свидетельства о рождении), данные справки по форме 2НДФЛ супруга(и) или иных членов семьи;
* сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
* сведения об идентификационном номере налогоплательщика;
* сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования);
* сведения, указанные в оригиналах и копиях приказов по персоналу Центра и материалах к ним, в том числе информация об отпусках, о командировках и т.п.;
* оригиналы приказов, изданных в Центре, и относящиеся к субъекту персональных данных, и материалы к данным приказам;
* сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) Работников Центра;
* материалы по аттестации и оценке Работников Центра;
* материалы по внутренним служебным расследованиям в отношении Работников Центра;
* сведения о временной нетрудоспособности Работников Центра;
* табельный номер Работника Центра;
* сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и иные сведения);
* сведения об административных наказаниях Работников за потребление наркотических средств без назначения врача:
* сведения об отсутствии судимости Работников Центра;
* иные сведения, с которыми Работник считает нужным ознакомить Работодателя.
1. **КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ**
	1. Документы, перечисленные в п.2.2. Положения, содержащие сведения о персональных данных Работников Центра, являются конфиденциальными. Центр обеспечивает конфиденциальность персональных данных, и обязана не допускать их распространения без согласия Работника, либо наличия иного законного основания.
	2. Все меры конфиденциальности при сборе, обработке и хранении персональных данных Работников распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
2. **ПРАВА И ОБЯЗАННОСТИ РАБОТОДАТЕЛЯ**
	1. Работодатель имеет право без согласия Работника осуществлять обработку его персональных данных в следующих случаях:
		1. если обработка персональных данных осуществляется на основании Трудового кодекса Российской Федерации и в целях исполнения трудового договора с Работником;
		2. если обработка персональных данных Работника осуществляется для статистических или иных научных целей при условии обязательного обезличивания его персональных данных;
		3. если обработка персональных данных Работника необходима для защиты жизни, здоровья или иных жизненно важных интересов Работника, если получение его согласия невозможно.
		4. в других случаях, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
		5. В иных случаях (не перечисленных в п.4.1. Положения) Работодатель может осуществлять обработку персональных данных Работника только с письменного согласия Работника. Согласие на обработку персональных данных по основаниям данного пункта может быть отозвано Работником. Обязанность предоставить доказательство получения согласия Работника на обработку его персональных данных по основаниям данного пункта, возлагается на Работодателя.
	2. Письменное согласие Работника на обработку своих персональных данных по основаниям пп.4.1.1. Положения должно включать в себя:
* фамилию, имя, отчество, адрес Работника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
* наименование и адрес Работодателя, получающего согласие Работника;
* цель обработки персональных данных;
* перечень персональных данных, на обработку которых дается согласие Работник;
* перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Работодателем способов обработки персональных данных;
* срок, в течение которого действует согласие, а также порядок его отзыва;
* личную подпись Работника.
	1. В целях обеспечения прав и свобод человека и гражданина Работодатель и его представители при обработке персональных данных Работника обязаны соблюдать следующие общие требования:
* Обработка персональных данных Работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия Работникам в трудоустройстве, обучения и продвижении в Центре, обеспечения личной безопасности Работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
* При определении объема и содержания персональных данных Работника, подлежащих обработке, Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» и иными федеральными законами.
	1. Работодатель не имеет права получать и обрабатывать персональные данные Работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации Работодатель вправе получать и обрабатывать данные о частной жизни Работника только с его письменного согласия.
	2. Работодатель не имеет права получать и обрабатывать персональные данные Работника о его членстве в организациях или его профсоюзной деятельности, за исключением случаев, предусмотренных действующим законодательством.
	3. Работодатель не должен запрашивать информацию о состоянии здоровья Работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения Работником трудовой функции.
	4. При принятии решений, затрагивающих интересы Работника, Работодатель не имеет права основываться на персональных данных Работника, полученных исключительно в результате их автоматизированной обработки.
	5. Защита персональных данных Работника от неправомерного их использования или утраты должна быть обеспечена Работодателем за счет средств Центра в порядке, установленном федеральным законодательством.
1. **ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА**
	1. Работник обязан передавать Работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации, настоящим Положением и Правилами внутреннего трудового распорядка, принятыми в Центре.
	2. Работник должен своевременно в срок, не превышающий пяти рабочих дней, сообщать Работодателю об изменении своих персональных данных.
	3. В целях обеспечения защиты персональных данных, хранящихся у Работодателя, Работник имеет право:
		1. На полную информацию о своих персональных данных и обработке этих данных; на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Работника, за исключением случаев, предусмотренных федеральным законом.

Сведения о наличии персональных данных должны быть предоставлены Работнику в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

* + 1. Определить своих представителей для защиты своих персональных данных.
		2. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона.
	1. Работник вправе требовать от Работодателя уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
	2. При отказе Работодателя исключить или исправить персональные данные Работника последний имеет право заявить в письменной форме Работодателю о своем несогласии с соответствующим обоснованием такого несогласия;

Персональные данные оценочного характера Работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

* 1. Требовать извещения Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные Работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.
	2. Обжаловать в суде любые неправомерные действия или бездействие Работодателя при обработке и защите его персональных данных.
	3. Передача информации третьей стороне возможна только при письменном согласии Работника, за исключением обстоятельств, установленных законодательством.
	4. Если Работник считает, что Работодатель осуществляет обработку его персональных данных с нарушением требований федерального законодательства или иным образом нарушает его права и свободы, Работник вправе обжаловать действия или бездействие Работодателя в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.
	5. Работник имеет право на сохранение и защиту своей личной и семейной тайны, на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.
	6. Во всех случаях отказ Работника от своих прав на сохранение и защиту конфиденциальности его персональных данных недействителен и юридически ничтожен.
1. **СБОР И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

6.1. Сбор персональных данных

– все персональные данные Работника Работодатель получает у него самого;

– если персональные данные Работника возможно получить только у третьей стороны, то Работник уведомляется об этом Работодателем заранее. Работодателем в этом случае должно быть получено письменное согласие Работника. Работодатель должен сообщить Работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и о последствиях отказа Работника дать письменное согласие на их получение;

– работник Центра предоставляет работнику отдела кадров достоверные сведения о себе. Информация, представляемая Работником при поступлении на работу в Центр, должна иметь документальную форму. Работник отдела кадров Центра проверяет достоверность сведений, сверяя данные, предоставленные Работником, с имеющимися у Работника документами.

6.2. При заключении трудового договора в соответствии со ст.65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет Работодателю:

* паспорт или иной документ, удостоверяющий личность;
* трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или Работник поступает на работу на условиях совместительства, либо трудовая книжка у Работника отсутствует в связи с ее утратой или по другим причинам;
* страховое свидетельство государственного пенсионного страхования;
* документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;
* документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;
* свидетельство о присвоении ИНН (при его наличии у работника);
* справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;
* cправку об административном наказании за потребление наркотических средств без назначения врача;
* Заключение предварительного медицинского осмотра Работника.

6.3. Документы, содержащие персональные данные Работника, создаются путём:

* создания комплекта документов, сопровождающих процесс оформления трудовых отношений Работника в Центре при его приеме, переводе и увольнении методом внесения сведений в учётные формы (на бумажных и электронных носителях);
* копирования оригиналов документов (документ об образовании, свидетельство ИНН, пенсионное свидетельство);
* получения оригиналов необходимых документов (трудовая книжка, личный листок по учёту кадров, автобиография).

6.4. При поступлении на работу в Центр:

* Работником отдела кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные Работника:

– общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные, сведения о месте жительства и контактных телефонах);

– сведения о воинском учете;

– данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

– сведения о переводах на другую работу;

– сведения об аттестации;

– сведения о повышении квалификации;

– сведения о профессиональной переподготовке;

– сведения о наградах (поощрениях), почетных званиях;

– сведения об отпусках;

– сведения о социальных гарантиях;

– сведения об изменении места жительства, контактных телефонов.

6.5. Личное дело Работника оформляется после издания приказа о приеме на работу.

- Все документы личного дела подшиваются в обложку образца, установленного в Центре. На ней указываются фамилия, имя отчество Работника, номер личного дела. К каждому личному делу прилагается фотография Работника размером 3х4.

- Все документы, поступающие в личное дело, располагаются в хронологическом порядке. Листы документов, подшитые в личное дело, нумеруются.

- Личное дело ведется на протяжении всей трудовой деятельности Работника в Центре. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

6.6. Хранение персональных данных

1. Персональные данные Работников могут храниться, как на бумажных носителях, так и в электронном виде.
2. В отделе кадров Центра хранятся в специально отведенных системах хранения (шкафах, сейфах) согласно приказу, определяющему места хранения носителей персональных данных следующие группы документов, содержащие данные Работников в единичном или сводном виде:
* документы, содержащие персональные данные Работников (комплекты документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекты документов по тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Центра, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие ведомства.
* документация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции Работников, приказы, распоряжения, указания руководства Центра); документы по планированию, учету, анализу и отчетности в части работы с персоналом Центра.
1. В том числе в специально отведенных системах хранения (шкафах, сейфах) согласно приказу, определяющему места хранения носителей персональных данных, хранятся:

- трудовые книжки, личные карточки Работников по форме Т-2;

- личные дела в бумажном виде в папках, прошитые и пронумерованные по страницам.

1. Личные файлы уволенных Работников хранятся в хранилище отдела кадров.
2. Ключи от шкафов, сейфов хранятся лично у начальника отдела кадров.

6.7. Персональные данные Работников могут также храниться в электронном виде в информационных системах персональных данных Центра, в электронных папках и файлах в ПК работников Центра.

Доступ к ПК строго ограничен кругом лиц, определённых приказом Главного врача Центра.

6.8. Хранение персональных данных в бухгалтерии:

* согласно приказу, определяющему места хранения носителей персональных данных, персональные данные, содержащиеся на бумажных носителях, хранятся в шкафах, сейфах согласно приказу, определяющему места хранения носителей персональных данных, установленных в служебных помещениях, занимаемых главным бухгалтером и иными работниками бухгалтерии.
* персональные данные, содержащиеся на электронных носителях информации, хранятся согласно приказу, определяющему места хранения носителей персональных данных.

6.10. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения.

6.11. Персональные данные, содержащиеся на электронных носителях информации, уничтожаются по акту по истечению установленного срока хранения.

**7. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ**

7.1. При передаче персональных данных Работника Работодатель должен соблюдать следующие требования:

- не сообщать персональные данные Работника третьей стороне без письменного согласия Работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья Работника, а также в случаях, установленных федеральным законом;

- предупредить лиц, получающих персональные данные Работника о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

- разрешать доступ к персональным данным Работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные Работника, которые необходимы для выполнения конкретных функций;

- передавать персональные данные Работника представителям Работников в порядке, установленном Трудовым кодексом Российской Федерации и Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», и ограничивать эту информацию только теми персональными данными Работника, которые необходимы для выполнения указанными представителями их функций.

7.2. Передача персональных данных Работника третьим лицам осуществляется только с письменного согласия Работника, которое оформляется по установленной форме (Приложение №1) и должно включать в себя:

- фамилию, имя, отчество, адрес Работника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование и адрес Работодателя, получающего согласие Работника;

- цель передачи персональных данных;

- перечень персональных данных, на передачу которых дает согласие Работник;

- срок, в течение которого действует согласие, а также порядок его отзыва.

* Согласия Работника на передачу его персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника; когда третьи лица оказывают услуги Работодателю на основании заключенных договоров, а также в случаях, установленных действующим законодательством и настоящим Положением.
* Работники Работодателя, передающие персональные данные Работников третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные работников. Акт составляется по установленной форме (Приложение №3), и должен содержать следующие условия:

- уведомление лица, получающего данные документы об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена;

- предупреждение об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами.

7.2. Передача документов (иных материальных носителей), содержащих персональные данные Работников, осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг Центру;

- соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных Работника;

- письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные Работника, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных Работника Центра несет начальник отдела кадров, а также работник, осуществляющий передачу персональных данных Работника третьим лицам.

7.3. Представителю Работника персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя Работника;

- письменного заявления Работника, написанного в присутствии работника отдела кадров Работодателя (если заявление написано Работником не в присутствии работника отдела кадров, то оно должно быть нотариально заверено).

Доверенности и заявления хранятся в отделе кадров в личном деле Работника.

7.4. Предоставление персональных данных Работника государственным органам производится в соответствии с требованиями действующего законодательства.

7.5. Персональные данные Работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого Работника, за исключением случаев, когда передача персональных данных Работника без его согласия допускается действующим законодательством Российской Федерации.

7.6. Сведения о работающем работнике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии письменного согласия Работника, удостоверенного нотариально.

7.7. Документы, содержащие персональные данные Работника, могут быть отправлены через организацию федеральной почтовой связи. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные, вкладываются в конверт вместе с сопроводительным письмом. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

**8. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКА**

8.1. Право доступа к персональным данным Работника в Центре имеют:

- Главный врач;

- начальник отдела кадров и работники отдела кадров;

- руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения);

- при переводе из одного структурного подразделения в другое, доступ к персональным данным Работника может иметь руководитель нового подразделения;

- сам Работник – субъект персональных данных;

- другие работники Центра при выполнении ими своих служебных обязанностей.

8.2. Перечень работников Центра, имеющих доступ к персональным данным Работников, определяется приказом Главного врача.

**9. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ**

9.1. Центр обязан, при обработке персональных данных, принимать необходимые организационные и технические меры для защиты персональных данных Работников от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

9.2. Защите подлежит:

- информация о персональных данных Работника, содержащаяся на бумажных носителях;

- документы, содержащие персональные данные Работника;

- персональные данные, содержащиеся на электронных носителях.

9.3. Общую организацию защиты персональных данных Работников по указанию Главного врача осуществляет назначенный работник, ответственный за организацию обработки персональных данных, и начальник отдела кадров в соответствии с должностными инструкциями.

9.4. Начальник отдела кадров обеспечивает:

- Ознакомление работника под роспись с настоящим Положением.

- Истребование с работников письменного обязательства о соблюдении конфиденциальности персональных данных Работника и соблюдении правил их обработки.

- Ознакомление работника под роспись с приказами и иными внутренними локальными нормативными актами, регулирующими обработку и защиту персональных данных в Центре.

- Общий контроль соблюдения Работниками мер по защите персональных данных.

9.5. Защита информационных систем Центра, в которых обрабатываются персональные данные Работников, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке, осуществляется в соответствии с Положением о мерах по организации защиты информационных систем персональных данных Центра.

9.6. Доступ к персональным данным Работника имеют работники Работодателя, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно перечню должностей.

В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией Главного врача, доступ к персональным данным Работника может быть предоставлен иному работнику, должность которого не включена в Перечень должностей работников, имеющих доступ к персональным данным Работника Центра, и которым они необходимы в связи с исполнением трудовых обязанностей.

9.6.1. Все работники, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных Работников (соглашение о неразглашении конфиденциальной информации).

Процедура оформления доступа к персональным данным Работника включает в себя:

- ознакомление Работника под роспись с настоящим Положением. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных Работника, с данными актами также производится ознакомление Работника под подпись.

- истребование с работника (за исключением Главного врача) письменного обязательства о соблюдении конфиденциальности персональных данных Работника и соблюдении правил их обработки, подготовленного по установленной форме.

9.6.2. Работник Работодателя, имеющий доступ к персональным данным Работников в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные Работника, исключающее доступ к ним третьих лиц.

В отсутствие работника на его рабочем месте не должно быть документов, содержащих персональные данные Работников.

- При уходе в отпуск, во время служебной командировки и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные Работников лицу, на которое локальным актом Центра (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей.

В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные Работников, передаются другому работнику, имеющему доступ к персональным данным Работников по указанию руководителя структурного подразделения.

9.6.3. При увольнении работника, имеющего доступ к персональным данным Работников, документы и иные носители, содержащие персональные данные Работников, передаются другому работнику, имеющему доступ к персональным данным Работников по указанию руководителя структурного подразделения или Главного врача.

9.6.4. Допуск к персональным данным Работника других работников Работодателя, не имеющих надлежащим образом оформленного доступа, запрещается.

9.7. Личные дела и документы, содержащие персональные данные Работников, хранятся в шкафах, сейфах, стеллажах и хранилищах, обеспечивающих защиту от несанкционированного доступа.

9.7.1. В Центре не допускается выдача личных дел работников на рабочие места руководителей. Личные дела могут выдаваться только Главному врачу. В исключительных случаях, по письменному разрешению Главного врача, - руководителю структурного подразделения (например, при подготовке материалов для аттестации Работника).

9.7.2. В конце рабочего дня все личные дела, выданные работникам, имеющим право доступа к этим документам, сдаются в отдел кадров.

 9.8. Защита доступа к электронным носителям, содержащим персональные данные Работников, обеспечивается, том числе:

* использованием лицензированных антивирусных и антихакерских программ, не допускающих несанкционированный доступ к персональным данным;
* разграничением прав доступа с использованием учетной записи;
* установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
* учетом машинных носителей персональных данных;
* обнаружением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;
* контролем эффективности принимаемых мер по обеспечению защищенности персональных данных.

9.9. Копировать и делать выписки персональных данных Работника разрешается исключительно в служебных целях с письменного разрешения начальника отдела кадров.

9.10. Ответы на письменные запросы других организаций и учреждений о персональных данных Работников Центра даются только с письменного согласия самого Работника, если иное не установлено законодательством. Ответы оформляются в письменном виде, на бланке Центра, и в том объеме, который позволяет не разглашать излишний объем персональных сведений о Работниках Центра.

9.11. Передача информации, содержащей сведения о персональных данных Работников Центра, по телефону, факсимильной связи, электронной почте запрещается.

10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

10.1. Главный врач, разрешающий доступ работника к документам, содержащим персональные данные Работника, несет персональную ответственность за данное разрешение.

10.2. Каждый работник Центра, получающий для работы документ, содержащий персональные данные Работника, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

10.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных Работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

10.4. За неисполнение или ненадлежащее исполнение Работником по его вине возложенных на него обязанностей по соблюдению установленного порядка обработки персональных данных Работников Работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

10.4.1. К лицам, виновным в нарушении норм, регулирующих получение, обработку и защиту персональных данных Работника, могут быть применены следующие дисциплинарные взыскания:

а) замечание;

б) выговор;

в) увольнение.

10.4.2. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

10.4.3. Приказ о применении к Работнику дисциплинарного взыскания с указанием оснований его применения объявляется Работнику под роспись в течение трех рабочих дней со дня его издания, не считая времени отсутствия работника на работе.

10.4.4. Если в течение года со дня применения дисциплинарного взыскания Работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Работодатель до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с Работника по собственной инициативе, по письменному заявлению Работника или по ходатайству его непосредственного руководителя.

10.5. Должностные лица, в обязанность которых входит ведение персональных данных работника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

10.6. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на Работников.

10.7. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

11. СПИСОК ИСПОЛЬЗОВАННЫХ ЗАКОНОДАТЕЛЬНЫХ И НОРМАТИВНЫХ АКТОВ

Разработка настоящего Положения осуществлена в соответствии со следующими нормативными документами:

Конституция Российской Федерации (часть 1 статьи 23, статья 24);

Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ;

Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;

постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

# ПОЛОЖЕНИЕ О МЕРАХ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

1. **ОСНОВНЫЕ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ**

В Положении используются следующие понятия, определения и сокращения:

**ПДн** - персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу - субъекту персональных данных.

**Обработка ПДн** - любое действие с персональными данными, совершаемое с использованием средств автоматизации или без использования таких средств.

**АИС** – информационная система персональных данных, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

**Автоматизированная обработка ПДн** – обработка ПДн с помощью средств вычислительной техники.

**Обработка ПДн без использования средств автоматизации** - 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.

**Актуальные угрозы безопасности персональных данных** - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

**Система защиты персональных данных** – **СЗПДн** - организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

**Закон «О персональных данных»** - Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

**Приказ ФСТЭК №17** - Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

**Приказ ФСТЭК №21** - Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
	1. Настоящее Положение о мерах по организации защиты информационных систем персональных данных в ОГБУЗ «Иркутский городской перинатальный центр» (далее – Положение) устанавливает состав и содержание организационных и технических мер по обеспечению безопасности в ОГБУЗ «Иркутский городской перинатальный центр» (далее – Центр) на протяжении всего цикла их создания и эксплуатации.

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой Центром в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 01.11.2012 г. №1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

* 1. Настоящее Положение является внутренним локальным актом Центра.

Настоящее Положение вступает в силу с момента его утверждения Главным врачом Центра и действует бессрочно, до замены его новым Положением.

Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля, а также в целях совершенствования технологий обработки ПДн.

Изменения к Положению утверждаются Главным врачом Центра.

* 1. Все работники Центра должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

Настоящее Положение является обязательным для исполнения всеми работниками Центра, имеющими доступ к АИС.

* 1. Ответственность за актуализацию настоящего Положения и текущий контроль над выполнением норм Положения возлагается на назначаемого приказом по Центру уполномоченного сотрудника, ответственного за обеспечение безопасности информационных систем персональных данных.
	2. Положение разработано с учетом требований Политики по защите персональных данных Центра. Центр учитывает требования настоящего Положения при разработке и утверждении внутренних локальных актов и иных документов Центра, связанных с обработкой ПДн.
1. **ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ**

3.1. В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической и видео информации), общесистемное, прикладное, специальное программное обеспечение, а также средства защиты информации.

3.2. Для обеспечения защиты информации, содержащейся в информационной системе, Центром назначается уполномоченный сотрудник ответственный за обеспечение безопасности информационных систем персональных данных.

3.3. Система защиты персональных данных включает в себя организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3.4. Выбор средств защиты информации для системы защиты персональных данных осуществляется Центром в соответствии с требованиями Приказов ФСТЭК России №17 и №21, а также иными нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю.

3.5. Определение типа угроз безопасности персональных данных, актуальных для информационных систем, производится Центром с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Закона «О персональных данных».

3.6. Центр обеспечивает классификацию информационных систем в зависимости от того, какие категории персональных данных в ней обрабатываются и какие типы угроз актуальны для АИС Центра. По результатам определяется набор требований, которые необходимо выполнить для обеспечения того уровня защищенности ПДн, который был определен при классификации АИС Центра.

3.7. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных и контроль за выполнением требований к защите ПДн при обработке их в АИС организуется и проводится Центром самостоятельно, не реже 1 раза в 3 года в сроки, определяемые Центром.

1. **ОСНОВНЫЕ МЕРЫ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**
	1. Состав и содержание организационных мер по обеспечению безопасности ПДн.

Необходимый уровень защищенности персональных данных при их обработке в информационных системах Центра обеспечивается принятием следующих основных организационных мер:

1. введение режима обеспечения безопасности помещений, в которых размещены АИС Центра, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения и обеспечивается Арендодателем;
2. обеспечение безусловной сохранности носителей персональных данных;
3. назначение уполномоченного сотрудника, ответственного за обеспечение безопасности информационных систем персональных данных Центра;
4. утверждение перечня персональных данных и иных объектов, подлежащих защите в АИС Центра;
5. утверждение перечня лиц, доступ которых к персональным данным, обрабатываемым в АИС Центра, необходим для выполнения ими служебных обязанностей;
6. проведение классификации АИС Центра, по результатам определяется набор требований, необходимых для обеспечения необходимого уровня защищенности ПДн;
7. обеспечение проведения не реже 1 раза в 3 года проверки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных, и осуществление регулярного контроля за выполнением требований к защите ПДн при обработке их в АИС.
	1. Мероприятия по реализации организационных мер по обеспечению безопасности ПДн.

С учетом требований, перечисленных в пункте 1 статьи 6 Положения, проводятся следующие мероприятия:

1. Приказом Главного врача назначается уполномоченный сотрудник, ответственный за обеспечение безопасности информационных систем персональных данных Центра. Разрабатывается и вводится в действие должностная инструкция, регламентирующая права и обязанности указанного сотрудника.
2. Вводится в действие приказ Главного врача «О создании Комиссии по персональным данным» (далее по тексту – Комиссия по персональным данным»).
3. Разрабатывается, утверждается и внедряется система организации доступа в помещения Центра, где осуществляется обработка ПДн, исключающая возможность несанкционированного доступа к техническим средствам обработки ПДн, хищения и нарушения работоспособности АИС, хищения носителей информации ПДн.
4. Вводится в действие инструкция о порядке организации внутриобъектового и пропускного режимов в помещениях Центра.
5. Определяются состав и категории обрабатываемых в Центре персональных данных (результат оформляется в виде локального нормативного акта с перечнем персональных данных и иных объектов, подлежащих защите в Центре).
6. Разрабатывается и вводится в действие инструкция пользователя АИС, регламентирующая права и обязанности работника Центра при работе с АИС.
7. Разрабатывается и вводится в действие локальный нормативный акт, регламентирующий разграничение прав доступа к обрабатываемым в АИС персональным данным.
8. Обеспечивается обучение Работников Центра, осуществляющих обработку ПДн в информационных системах персональных данных, предусматривающее проведение не реже одного раза в год обучения пользованию средствами защиты информации, которые применяются в информационных системах Центра, правилам работы с ними, правилам обработки ПДн, в соответствии с утвержденными в Центре требованиями.
9. Разрабатывается и вводится в действие инструкция о порядке учета, использования, транспортировки, хранения и уничтожения в Центре съемных носителей персональных данных.
10. Обеспечивается учет съемных носителей ПДн в каждом структурном подразделении Центра (вводятся в действие журналы учета съемных носителей ПДн).
11. Локальными актами, регламентирующими обработку и защиту персональных данных работников Центра, утверждаются перечни подразделений и работников, допущенных к обработке ПДн в информационных системах Центра.
12. Принимается локальный нормативный акт об ответственности работников Центра за разглашение персональных данных и несанкционированный доступ к персональным данным в информационных системах Центра.
13. Комиссией по персональным данным проводятся внутренние проверки и классификация АИС Центра. Результаты оформляются в виде письменных отчетов, на основании которых разрабатывается план мероприятий по обеспечению безопасности ПДн в АИС Центра.
14. Разрабатывается и утверждается план внутренних проверок состояния защиты ПДн в Центре. Вводится в действие журнал учета мероприятий по контролю соблюдения режима защиты персональных данных в информационных системах Центра.
	1. Технические меры по обеспечению безопасности ПДн в АИС.

Центр принимает технические меры по обеспечению безопасности информационных систем персональных данных.

План мероприятий по обеспечению защиты персональных данных в Центре включает следующие этапы работы:

1. определение на основании Приказов ФСТЭК России №17 и №21 базового набора мер по обеспечению безопасности персональных данных в АИС Центра;
2. адаптация базового набора мер под АИС Центра с учетом особенностей их функционирования, исключая те меры, которые связаны с информационными технологиями, не используемыми в АИС;
3. уточнение списка мер с включением в него не выбранных ранее мер для нейтрализации актуальных угроз;
4. внедрение дополнительных мер, обеспечивающих выполнение требований к защите персональных данных, установленных нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

В составе мер, входящих в план мероприятий по обеспечению защиты персональных данных в Центре, в том числе, предусматривается:

1. внедрение системы парольной аутентификация работников Центра, допущенных к работе с АИС, предусматривающей определение минимальной длинны пароля, управление сроком действия и периодической сменой паролей; ограничение числа неудачных попыток входа в систему и использование программных генераторов паролей;
2. установление инструктивных и технических правил, обеспечивающих разграничение прав доступа работников к различным ПДн, находящимся в АИС Центра;
3. разработка и внедрение регламента, обеспечивающего установку и запуск в АИС только разрешенного к использованию в информационной системе программного обеспечения, и исключающего возможность использования, запрещенного к использованию в информационной системе программного обеспечения;
4. разработка инструкции, регламентирующей порядок резервирования и восстановления работоспособности программного обеспечения, баз данных и систем защиты АИС;
5. внедрение технологий, позволяющих осуществлять резервирование и восстановление работоспособности программного обеспечения, баз данных и систем защиты АИС;
6. разработка инструкции, регламентирующей модификацию программного обеспечения и технических средств информационной системы персональных данных;
7. внедрение технологий, позволяющих осуществлять сбор, запись, хранение, анализ, просмотр и защиту информации о событиях безопасности в АИС Центра;
8. использование программного обеспечения по антивирусной защите, обеспечивающего обнаружение в АИС вредоносных программ, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования ПДн, иной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;
9. проведение систематических мероприятий по анализу защищенности АИС и тестированию работоспособности системы защиты персональных данных;
10. обеспечение защиты АИС, ее средств, систем связи и передачи данных при взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями;
11. разработка и ввод в действие электронного журнала учета обращений субъектов персональных данных о выполнении их законных прав, при обработке данных в АИС.

4.4 Предоставление пользователями (посетителями) официального сайта Центра сведений, содержащих персональные данные, осуществляется в соответствии с требованиями, размещенными на официальном сайте Центра (https://www.irgpc.ru/).

1. **ЛИЦА, ОТВЕТСТВЕННЫЕ ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**
	1. Общее руководство деятельностью Центра по обеспечению безопасности ПДн осуществляет Главный врач.
	2. Главный врач приказом назначает уполномоченного сотрудника, ответственного за обеспечение безопасности АИС в Центре.
	3. Уполномоченный сотрудник, ответственный за обеспечение безопасности АИС в Центре, получает указания непосредственно от Главного врача.
	4. Уполномоченный сотрудник, ответственный за обеспечение безопасности АИС в Центре, обязан не реже одного раза в три года проводить проверку состава и структуры АИС, состава угроз безопасности ПДн в АИС и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных, при необходимости вносить предложения по доработке или модернизации системы защиты ПДн.
	5. Главный врач приказом создает в Центре Комиссию по персональным данным, на которую возлагаются следующие обязанности:
2. реализация мероприятий, предусмотренных настоящим Положением;
3. осуществление внутреннего контроля и аудита соответствия практики обработки персональных данных в Центре тем требованиям и нормам, которые установлены Законом «О персональных данных», а также принятым в этой сфере иным нормативным правовым актам и требованиям к защите персональных данных, и локальным нормативным актам Центра;
4. организационное, методическое и научно-техническое руководство работами по созданию либо модернизации системы защиты ПДн.
	1. Центр на договорной основе имеет право привлечь для разработки и внедрения систем защиты ПДн в АИС Центра специализированные организации, имеющие лицензии ФСТЭК, ФСБ России на соответствующие виды деятельности.
5. **ПОРЯДОК МОДЕРНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ПДн**
	1. Для АИС, находящихся в эксплуатации, модернизация или доработка системы защиты ПДн должна проводиться в следующих случаях:
6. изменение состава или структуры самой АИС или технических особенностей ее построения (изменение состава или структуры программного обеспечения, технических средств обработки ПДн, топологии АИС);
7. изменение состава угроз безопасности ПДн в АИС;
8. изменение уровня защищенности, который необходимо обеспечить при защите ПДн.
	1. Для определения необходимости доработки или модернизации систем защиты ПДн не реже одного раза в три года должна проводиться проверка состава и структуры АИС, состава угроз безопасности ПДн в АИС и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных. Проверка проводится уполномоченным сотрудником, ответственным за обеспечение безопасности АИС. Результаты проверки оформляются Отчетом по проведению внутренней проверки и утверждаются Главным врачом.
9. **КОНТРОЛЬ СОБЛЮДЕНИЯ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СИСТЕМ ЗАЩИТЫ ПДн**
10. Уполномоченный сотрудник, ответственный за обеспечение безопасности АИС, и Комиссия по персональным данным периодически (не реже одного раза в год) должны проводить проверку соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.
11. В случае выявления фактов несоблюдения условий хранения носителей ПДн, или использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности ПДн, либо нарушения заданного уровня безопасности ПДн, должно в обязательном порядке проводиться разбирательство (внутренняя проверка).
12. В процессе проведения разбирательства необходимо провести разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.
13. По окончании проведения разбирательства готовится заключение о лицах, виновных в выявленных нарушениях.

# ПОЛОЖЕНИЕ О НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

* 1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», и устанавливает единый порядок неавтоматизированной обработки персональных данных в ОГБУЗ «Иркутский городской перинатальный центр» (далее – Центр).
	2. В целях настоящего Положения используются следующие термины и понятия:

 - персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

 - обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, уничтожение персональных данных;

- 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.

1.3. Задачи, решаемые в процессе обработки персональных данных:

- документационное обеспечение обработки персональных данных;

- защита документированной информации, содержащей персональные данные.

1. **ОСНОВНЫЕ УСЛОВИЯ ПРОВЕДЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**
2. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных статьей 6 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»;

- после направления уведомления об обработке персональных данных в Центре, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»;

- после принятия необходимых мер по защите персональных данных.

1. В Центре приказом Главного врача назначается работник, ответственный за организацию обработки и защиту персональных данных, и определяется перечень лиц, допущенных к обработке персональных данных.
2. Работники, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением.
3. Запрещается обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке.
4. **СИСТЕМА ДОСТУПА К КОНФИДЕНЦИАЛЬНЫМ ДОКУМЕНТАМ**
5. Система доступа представляет собой совокупность норм и правил, определяющих порядок предоставления работникам прав доступа документам, содержащим конфиденциальную информацию.
6. Система доступа должна отвечать следующим требованиям:

- доступ к конфиденциальным документам может предоставляться работникам, письменно оформившим с Центром соглашение о неразглашении ставших им известными конфиденциальных сведений. Письменное оформление соглашения о неразглашении конфиденциальной информации (соблюдения режима конфиденциальности) является обязательным условием для доступа работников к документам;

- доступ к конфиденциальным документам должен быть обоснованным, т.е. базироваться на служебной необходимости ознакомления с конкретным документом именно данного работника;

- система доступа должна давать возможность обеспечивать работников всеми необходимыми им в силу служебных обязанностей документами, но только теми, которые действительно необходимы для выполнения конкретного вида работ;

- доступ к документам должен быть санкционированным, т.е. осуществляться только по соответствующему разрешению уполномоченного на то должностного лица. При этом соответствующее должностное лицо может давать разрешение на ознакомление с документами, только входящими в сферу его деятельности и только установленному кругу лиц;

- доступ к документам осуществляется согласно должностной инструкции.

3.3. Доступ работников Центра к конфиденциальной информации осуществляется на добровольной основе. Эти отношения устанавливаются при приеме гражданина на работу или уже в ходе трудовых отношений. При этом соблюдаются следующие условия:

- ознакомление работника под роспись с перечнем конфиденциальной информации;

- ознакомление работника под роспись с установленным в Центре режимом по охране конфиденциальности и с мерами ответственности за его нарушение;

- создание работнику необходимых условий для соблюдения им установленного режима по охране конфиденциальности.

3.4. Доступ работников Центра к персональным данным осуществляется в соответствии с Перечнем допущенных к обработке персональных данных в Центре.

3.5. Работник принимает следующие обязательства:

- по соблюдению установленного в Центре режима по охране конфиденциальной информации;

- о неразглашении конфиденциальной информации, ставшей ему известной в период выполнения трудовых отношений, после прекращения трудового договора в течение срока, предусмотренного в Соглашении о неразглашении конфиденциальной информации и не использовании этой информации в личных целях;

- о возмещении причиненного ущерба, если работник виновен в разглашении конфиденциальной информации, ставшей ему известной в связи с выполнением им трудовых обязанностей (в том числе после прекращения трудового договора);

* о возврате при прекращении или расторжении трудового договора всех имеющихся у работника материальных носителей конфиденциальной информации.
1. **ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ**

4.1. На бумажных носителях:

4.1.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных и магнитных носителях.

* + 1. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.
		2. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

* + 1. 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.

* + 1. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на объекты Центра или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом Центра, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на объекты Центра.

* + 1. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

* + 1. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).
		2. Правила, предусмотренные пунктами 4.1.6 и 4.1.7 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.
		3. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

4.2. В электронном виде без использования средств автоматизации:

* + 1. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на электронных носителях информации.
		2. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных.
		3. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от иных зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

1. **ПОДГОТОВКА И УЧЕТ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ**
	1. Бланки типовых форм документов (справки, карточки, талоны, ведомости и т.п.) могут изготавливаться при помощи средств вычислительной техники или на компьютере.
	2. Персональные данные (переменная часть) в типовые формы документов вносятся при помощи средств вычислительной техники, рукописным способом.
	3. После внесения переменной части в типовые формы, последние становятся документами и подлежат немедленному учету в журнале изданных документов с присвоением им учетного номера.
2. **ПОЛУЧЕНИЕ (ОТПРАВЛЕНИЕ) ДОКУМЕНТОВ И ИХ УЧЕТ**

6.1. Все документы, поступающие из иных организаций, подлежат регистрации в журнале учета поступивших документов. На самом документе в правом нижнем углу первого листа документа проставляется отметка о поступлении, которая содержит входящий номер, присвоенный документу, дату поступления.

6.2. Пересылка документов может осуществляться через органы специальной связи или через почтовое отделение связи.

6.3. Об отправленных документах производятся соответствующие отметки в учетных формах.

1. **КОПИРОВАНИЕ ДОКУМЕНТОВ**
	1. При действительной служебной необходимости в дополнительных экземплярах документов производится их копирование.
	2. На некоторых документах может стоять отметка о том, что снятие копий с этого документа не разрешается. Такие документы копированию не подлежат.
	3. Разрешение на копирование (снятие копий) документов могут давать соответствующие должностные лица (руководители структурных подразделений), наделенные правом распоряжения сведениями.
	4. Разрешение на изготовление дополнительных экземпляров (копий) учтенного документа оформляется на обороте последнего листа экземпляра, с которого производится копирование. В разрешении указываются номера документов или страниц, с которых необходимо сделать копию, а также количество копий.
2. **РЕЖИМ СОХРАННОСТИ ДОКУМЕНТОВ**
	1. Организация хранения документов предполагает, что помещения, где хранятся документы, должны соответствовать требованиям технической безопасности, противопожарной безопасности, а также установленным санитарным нормам.
	2. Для обеспечения физической сохранности документов, дел, а также для предотвращения разглашения содержащейся в них информации устанавливается специальный режим их хранения и обращения.
	3. Право входа в такие помещения имеют Главный врач Центра и работники, имеющие прямое отношение к обработке и хранению документов.

# НОРМАТИВНЫЕ И МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ

При организации и проведении работ по обеспечению безопасности ПДн в Центре, субъекты ПДн должны руководствоваться следующими нормативными и методическими документами:

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. Федеральный закон от 19.12.2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы «О защите физических лиц при автоматической обработке персональных данных»;
4. Указ Президента Российской Федерации от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
5. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
6. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
7. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требования к защите персональных данных при их обработке в информационных системах персональных данных»;
8. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
9. Политика по защите персональных данных;