Приложение №1 к приказу
ГБУЗ РК «Республиканская больница им. В.А. Баранова
№404 от «02» августа 2023

УТВЕРЖДАЮ

Главный врач ГБУЗ РК «Республиканская больница им. В.А. Баранова»
_____ Карапетян Т.Д.

Политика информационной безопасности систем персональных данных в ГБУЗ РК «Республиканская больница им. В.А. Баранова»

(Приложение №1 к Приказу главного врача №404 от «02» августа 2023г.)

Петрозаводск
2023

Содержание

1. Общие положения

1.1. Основные понятия, используемые в Политике в отношении обработки персональных данных в ГБУЗ РК «Республиканская больница им. В.А. Баранова»:

- **персональные данные (далее — ПДн)** – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);
- **оператор** персональных данных (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- **обработка** персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования.
- **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;
- **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- **блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- **уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- **информационная система персональных данных (далее – ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- **субъект персональных данных.** Физическое лицо, данные которого обрабатываются;
- **конфиденциальность персональных данных.** Обязательное для оператора и иных лиц, получивших доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные.

Обозначения и сокращения

АВС – антивирусные средства
АРМ - автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИСПДн –информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие

ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

1.2. Политика в отношении обработки персональных данных (далее - Политика) направлена на защиту прав и свобод физических лиц, персональные данные которых обрабатывает ГБУЗ ГБУЗ РК «Республиканская больница им. В.А. Баранова» (далее - Оператор).

1.3. Политика разработана в соответствии с п. 2 ч.1 ст. 18.1 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее - ФЗ «О персональных данных»), а также в соответствии с Федеральным законом от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности».

1.4. Политика содержит сведения, подлежащие раскрытию в соответствии с ч. 1 ст. 14 ФЗ «О персональных данных», и является общедоступным документом.

2. Правовые основания обработки персональных данных

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности ИСПДн ГБУЗ РК «Республиканская больница им. В.А. Баранова» (далее – ГБУЗ РК РБ). Кроме того, обработка персональных данных Оператором осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Оператор выступает в качестве работодателя (гл. 14 ТК РФ), в связи с реализацией Оператором своих прав и обязанностей как юридического лица.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн ГБУЗ РК РБ.

Обработка персональных данных в учреждении осуществляется в связи с выполнением Оператором функций, предусмотренных его учредительными документами и определяемых следующими нормативными правовыми актами РФ:

- Конституцией Российской Федерации
- Трудовым кодексом Российской Федерации
- Гражданским кодексом Российской Федерации
- Федеральным законом от 19.12.2005 г. №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»
- Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных»
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Федеральным законом от 21.11.2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»
- Постановлением Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Постановлением Правительства РФ от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- Федеральный закон от 14.07.2022 № 266-ФЗ "О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности».
- «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Заместителем директора ФСТЭК России от 15.02.2008 г.,
- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.
- «Методических рекомендаций для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости» Министерства здравоохранения и социального развития РФ от 23.12.2009 г.
- иными нормативными актами Российской Федерации

Кроме того, обработка персональных данных Оператором осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Оператор

выступает в качестве работодателя (гл. 14 ТК РФ), в связи с реализацией Оператором своих прав и обязанностей как юридического лица.

3. Цели обработки персональных данных

- Обеспечение наиболее полного исполнения обязательств и компетенций в соответствии с законом от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными постановлением Правительства РФ от 4 октября 2012 г. №1006;
- осуществление деятельности учреждения согласно действующему законодательству Российской Федерации и уставу Оператора;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

Цель №1: Установление медицинского диагноза, оказание медицинских медико-социальных услуг. **Категории субъектов**: законные представители, иные категории субъектов персональных данных, персональные данные которых обрабатываются; физические лица, обратившиеся за медицинской помощью (пациенты). **Категория данных**: общие персональные данные, специальные персональные данные. **Способ обработки персональных данных**: автоматизированная обработка, с передачей по внутренней сети юридического лица, с передачей по сети Интернет, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование. **Срок или условие прекращения обработки персональных данных:** по истечении 25 лет с момента последнего обращения за медицинской помощью. **Уничтожение персональных данных** на бумажных носителях подтверждается специальным актом об уничтожении. Уничтожение ПДн с использованием компьютерной техники, по завершении уничтожения данных представляется соответствующий акт, и выгрузка из журнала регистрации событий в информационной системе персональных данных.

Цель №2: Ведение кадрового и бухгалтерского учёта. **Категории субъектов**: работники. **Категория данных**: общие персональные данные. **Способ обработки персональных данных**: автоматизированная обработка, с передачей по внутренней сети юридического лица, с передачей по сети Интернет, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование. **Срок или условие прекращения обработки персональных данных:** Хранение ПДн осуществляется до достижения целей обработки персональных данных (например, до истечения срока действия ранее исполненного договора); при отзыве субъектом персональных данных согласия на обработку его персональных данных. **Уничтожение персональных данных** на бумажных носителях подтверждается специальным актом об уничтожении. Уничтожение ПДн с использованием компьютерной техники, по завершении уничтожения данных представляется соответствующий акт, и выгрузка из журнала регистрации событий в информационной системе персональных данных.

Цель №3: Электронная запись на приём к врачам специалистам на сайте ГБУЗ РК «Республиканская больница им. А.В. Баранова». **Категории субъектов**: Законные представители, иные категории субъектов персональных данных, персональные данные которых обрабатываются; физические лица, обратившиеся за медицинской помощью (пациенты). **Категория данных**: общие персональные данные. **Способ обработки персональных данных**: автоматизированная обработка, с передачей по внутренней сети юридического лица, с передачей по сети Интернет, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование. **Срок или условие прекращения обработки персональных данных:** Хранение ПДн осуществляется до достижения целей обработки персональных данных; при отзыве субъектом персональных данных согласия на обработку его персональных данных. **Уничтожение персональных данных** на бумажных носителях подтверждается специальным актом об уничтожении. Уничтожение ПДн с использованием компьютерной техники, по завершении уничтожения данных представляется соответствующий акт, и

выгрузка из журнала регистрации событий в информационной системе персональных данных. Срок или условие прекращения обработки персональных данных: по истечении 25 лет с момента последнего обращения за медицинской помощью.

4. Сведения об обработке персональных данных

4.1 Оператор обрабатывает персональные данные на законной и справедливой основе для выполнения возложенных законодательством функций, полномочий и обязанностей, осуществления прав и законных интересов Оператора, работников Оператора и третьих лиц.

4.2 На основании норм Трудового кодекса РФ (ст. 86), а также исходя из положений ст. 6, ст. 9 ФЗ «О персональных данных», обработка персональных данных Оператором осуществляется:

- с согласия субъекта персональных данных на обработку его персональных данных;
- в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;
- с согласия наследников субъекта персональных данных, если такое согласие не было дано субъектом персональных данных в случае смерти субъекта персональных данных;
- с согласия законного представителя субъекта персональных данных в случае недееспособности субъекта персональных данных.

4.3 Оператором обрабатываются персональные данные следующих субъектов:

- физические лица, состоящие с Оператором в трудовых отношениях;
- физические лица, являющиеся близкими родственниками работников Оператора;
- физические лица, прервавшие трудовые отношения с Оператором;
- физические лица, являющиеся соискателями вакантных должностей (далее - соискатели);
- физические лица, состоящие с Оператором в гражданско-правовых отношениях;
- физические лица, персональные данные которых необходимы в целях оказания услуг, оказываемых в соответствии с учредительными документами Оператора (далее - граждане).

Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку (Приложение №_____ к приказу ГБУЗ РБ от _____ года № _____).

4.4 Персональные данные, обрабатываемые Оператором:

- полученные при осуществлении трудовых отношений;
- полученные для осуществления отбора кандидатов на работу;
- полученные при осуществлении гражданско-правовых отношений;
- полученные при оказании услуг в соответствии с уставом Оператора. Полный список персональных данных представлен в перечне сведений конфиденциального характера, утвержденном Оператором.

4.5 Оператор получает персональные данные непосредственно у субъекта персональных данных или от его законного представителя.

4.6 Оператор обрабатывает персональные данные автоматизированным и неавтоматизированным способами.

4.7 Действия по обработке персональных данных включают сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование,

передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение.

4.8 К обработке персональных данных в организации допускаются только сотрудники, прошедшие определенную процедуру допуска, к которой относятся:

- ознакомление сотрудника с локальными нормативными актами Оператора (положения, инструкции и т.д.), строго регламентирующими порядок и процедуру работы с персональными данными;
- взятие с сотрудника подписки о соблюдении конфиденциальности в отношении персональных данных при работе с ними;

4.9 Сотрудники, имеющие доступ к персональным данным, получают только ту информацию, которая необходима им для выполнения конкретных трудовых функций.

5. Обработка персональных данных работников

5.1 Оператор обрабатывает персональные данные работников Оператора в рамках правоотношений, урегулированных Трудовым кодексом РФ от 30 декабря 2001 г. №197-ФЗ (далее - ТК РФ), в том числе главой 14 ТК РФ, касающейся защиты персональных данных работников.

5.2 Оператор обрабатывает персональные данные работников с целью выполнения трудовых договоров, соблюдения норм законодательства РФ, а также с целью:

- вести кадровый учет
- вести бухгалтерский учет
- осуществлять функции, полномочия и обязанности, возложенные законодательством РФ на Оператора, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд РФ, в Фонд социального страхования РФ, в Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы;
- соблюдать нормы и требования по охране труда и обеспечения личной безопасности работников организации, сохранности имущества;
- контролировать количество и качество выполняемой работы;
- предоставлять льготы и компенсации, предусмотренные законодательством РФ;
- открывать личные банковские счета работников организации для перечисления заработной платы;
- организовывать обучение работников организации

5.3 Оператор не принимает решения, затрагивающие интересы работников, основываясь на их персональных данных, полученным электронным образом или исключительно в результате автоматизированной обработки.

5.4 Оператор защищает персональные данные работников в порядке, установленном ТК РФ, ФЗ «О персональных данных» и иными федеральными законами.

5.5 Оператор знакомит работников и их представителей под подпись с документами, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

5.6 Оператор разрешает доступ к персональным данным только допущенным лицам, которые имеют право получать те данные, которые необходимы для выполнения их функций.

5.7 Оператор получает все персональные данные работников у них самих. Если данные работника возможно получить только у третьей стороны, Оператор заранее уведомляет об этом работника и получает его письменное согласие. Оператор сообщает работнику о целях, источниках, способах получения, а также о характере подлежащих получению данных и последствиях отказа работника дать письменное согласие на их получение.

5.8 Работники Оператора, передающие персональные данные работников третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные субъектов. Акт 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.

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

- договора на оказание услуг Оператора;
- 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.

5.10 Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных работника несет сотрудник Оператора, осуществляющий передачу персональных данных работника третьим лицам.

5.11 Представителю работника (в том числе адвокату) персональные данные передаются в порядке, установленном действующим законодательством и настоящей Политикой. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя работника;
- письменного согласия работника, написанного в присутствии работника ответственного за организацию обработки персональных данных, (если согласие написано работником не в присутствии работника ответственного за организацию обработки персональных данных, то оно должно быть нотариально заверено).

5.12 Предоставление персональных данных работника государственным органам производится в соответствии с требованиями действующего законодательства и настоящей Политикой.

5.13 Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного согласия самого работника, за исключением случаев, когда передача персональных данных работника без его согласия допускается действующим законодательством РФ.

5.14 Оператор обрабатывает персональные данные работников в течение срока действия трудового договора. Оператор обрабатывает персональные данные уволенных работников в течение срока, установленного п.5 ч.3 ст.24 части первой Налогового кодекса РФ от 31.07.1998 г. №146-ФЗ, ч.1 ст.29 Федерального закона «О бухгалтерском учете» от 06.12.2011 г. №402-ФЗ и иными нормативными правовыми актами.

5.15 Оператор может обрабатывать специальные категории персональных данных работников (сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения им трудовых функций) на основании п.2.3 ч.2 ст10 ФЗ «О персональных данных»

5.16 Оператор обрабатывает следующие персональные данные работников:

- фамилия, имя отчество;
- дата, месяц, год рождения;
- место рождения;
- гражданство;
- национальная принадлежность;
- образование;
- профессия;
- трудовой стаж;

- семейное положение;
- состав семьи;
- тип, серия, номер, дата выдачи, информация о выдавшем органе документа, удостоверяющего личность;
- доходы;
- данные о социальных льготах;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования;
- должность;
- страховые взносы на ОМС;
- страховые взносы на ОПС;
- налоговые вычеты;
- выход на пенсию;
- сведения о состоянии здоровья;
- сведения о воинском учете;
- данные о приеме на работу;
- 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;
- адрес
- номер контактного телефона, адрес электронной почты (по желанию);

5.17 Оператор не сообщает третьей стороне персональные данные работника без его письменного согласия, кроме случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных ТК РФ, ФЗ «О персональных данных» или иными федеральными законами.

5.18 Оператор не сообщает персональные данные работника в коммерческих целях без его письменного согласия.

5.19 Оператор передает персональные данные работников их представителям в порядке, установленном ТК РФ, ФЗ «О персональных данных» и иными федеральными законами, и ограничивает эту информацию только теми данными, которые необходимы для выполнения представителями их функций.

5.20 Оператор предупреждает лиц, получающих персональные данные работника, что эти данные могут быть использованы только в целях, для которых они сообщены, требует от этих лиц подтверждения, что это правило соблюдено.

5.21 В порядке, установленном законодательством, и в соответствии со ст.7 ФЗ «О персональных данных» для достижения целей обработки персональных данных и с согласия работников Оператор предоставляет персональные данные работников или поручает их обработку следующим лицам:

- Государственные органы (ПФР, ФНС, ФСС, ФОМС, военные комиссариаты, профсоюзные органы, предусмотренные действующим законодательством РФ и др.);
- Банк (в рамках зарплатного проекта);
- Министерство здравоохранения Республики Карелия (в рамках получения

квалификационной категории).

5.22 Работник может получить свободный бесплатный доступ к информации о его персональных данных и об обработке этих данных. Работник может получить копию любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральным законом.

5.23 Работник может получить доступ к медицинской документации, отражающей состояние его здоровья, с помощью медицинского работника по его выбору.

5.24 Работник может исключить или исправить свои неверные или неполные персональные данные, а также данные, обработанные с нарушением требований ТК РФ, ФЗ «О персональных данных» или иного федерального закона. При отказе Оператора исключить или исправить персональные данные работника он может заявить в письменной форме о своем несогласии и обосновать такое несогласие.

5.25 Работник может требовать известить всех лиц, которым ранее были сообщены его неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях иди дополнениях.

5.26 Работник может обжаловать в суд любые неправомерные действия или бездействие Оператора при обработке и защите его персональных данных.

6. Обработка персональных данных близких родственников работников

6.1 Оператор обрабатывает персональные данные близких родственников работников Оператора с целью выполнения трудовых договоров, соблюдения норм законодательства РФ, а также с целью:

- вести кадровый учет
- вести бухгалтерский учет

6.2 Оператор обрабатывает персональные данные близких родственников работников Оператора в объеме, предусмотренном унифицированной формой № Т-2, утвержденной постановлением Госкомстата Российской Федерации от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», либо в случаях, установленных законодательством Российской Федерации (получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат).

7. Обработка персональных данных сотрудников по договорам гражданско-правового характера

7.1 Оператор обрабатывает персональные данные сотрудников по договорам гражданско-правового характера в рамках правоотношений с Оператором, урегулированных частью второй Гражданского кодекса Российской Федерации от 26.01.1996 г. №14-ФЗ.

7.2 Оператор обрабатывает персональные данные сотрудников по договорам гражданско-правового характера в целях соблюдения норм законодательства РФ, а также заключает и выполняет договора гражданско-правового характера.

7.3 Оператор обрабатывает персональные данные сотрудников по договорам гражданско-правового характера с их согласия, предоставляемого на срок действия заключенных с ними договоров. В случаях, предусмотренных ФЗ «О персональных данных», согласие предоставляется в письменном виде. В иных случаях согласие считается полученным при заключении договора или при совершении конклюдентных действий.

7.4 Оператор обрабатывает персональные данные сотрудников по договорам гражданско-правового характера в течение сроков действия, заключенных с ними договоров. Оператор может обрабатывать персональные данные сотрудников по договорам гражданско-правового характера после окончания сроков действия заключенных с ними договоров в течение срока, установленного п.5 ч.3 ст.24 части первой Налогового кодекса РФ от 31.07.1998 г. №146-ФЗ, ч.1 ст.29 Федерального закона «О бухгалтерском учете» от 06.12.2011 г. №402-ФЗ и иными нормативными правовыми актами.

7.5 Оператор обрабатывает следующие персональные данные сотрудников по договорам гражданско-правового характера:

- фамилия, имя отчество;
- дата, месяц, год рождения;
- место рождения;
- тип, серия, номер, дата выдачи, информация о выдавшем органе документа, удостоверяющего личность;
- адрес;
- номер страхового свидетельства государственного пенсионного страхования;
- должность;
- идентификационный номер налогоплательщика;
- доходы;
- страховые взносы на ОМС;
- страховые взносы на ОПС;
- номер контактного телефона, адрес электронной почты (по желанию).

7.6 В порядке, установленном законодательством, и в соответствии со ст.7 ФЗ «О персональных данных» для достижения целей обработки персональных данных и с согласия работников Оператор предоставляет персональные данные сотрудников по договору гражданско-правового характера или поручает их обработку следующим лицам:

- Государственные органы (ПФР, ФНС, ФСС, и др.)
- Банк (для начисления вознаграждения за выполненные работы/оказанные услуги)

8. Обработка персональных данных граждан (по договорам)

8.1 Оператор обрабатывает персональные данные граждан в рамках правоотношений с Оператором, урегулированных частью второй Гражданского Кодекса Российской Федерации от 26.01.1996 г. №14-ФЗ.

8.2 Оператор обрабатывает персональные данные граждан в целях соблюдения норм законодательства РФ, а также с целью:

- заключать и выполнять обязательства по договорам с гражданами;
- осуществлять виды деятельности, предусмотренные учредительными документами Оператора.

8.3 Оператор обрабатывает персональные данные граждан с их согласия, предоставляемого на срок действия заключенных с ними договоров. В случаях, предусмотренных ФЗ «О персональных данных», согласие предоставляется в письменном виде. В иных случаях согласие считается полученным при заключении договора или при совершении конклюдентных действий.

8.4 Оператор обрабатывает персональные данные граждан в течение сроков действия, заключенных с ними договоров. Оператор может обрабатывать персональные данные граждан после окончания сроков действия заключенных с ними договоров в течение срока, установленного п.5 ч.3 ст.24 части первой Налогового кодекса РФ от 31.07.1998 г. №146-ФЗ, ч.1 ст.29 Федерального закона «О бухгалтерском учете» от 06.12.2011 г. №402-ФЗ и иными нормативными правовыми актами.

8.5 Оператор обрабатывает следующие персональные данные граждан:

- фамилия, имя, отчество;
- тип, серия, номер, дата выдачи, информация о выдавшем органе документа, удостоверяющего личность;
- адрес;
- дата, месяц, год рождения;
- сведения о профессиональной деятельности;
- номер контактного телефона, адрес электронной почты (по желанию);
- информация о состоянии здоровья;
- другая информация, необходимая для правильного проведения и интерпретации медицинских исследований;
- результаты выполненных медицинских исследований.

9. Обработка персональных данных соискателей

9.1 Оператор обрабатывает персональные данные соискателей.

9.2 Оператор обрабатывает персональные данные соискателей с целью:

- принимать решения о приеме либо отказе в приеме на работу.

9.3 Оператор обрабатывает персональные данные соискателей с их письменного согласия, предоставляемого на срок, необходимый для принятия решения о приеме, либо отказе в приеме на работу. Исключение составляют случаи, когда от имени соискателя действует кадровое агентство, с которым он заключил соответствующий договор, а также при самостоятельном размещении соискателем своего резюме, доступного неограниченному кругу лиц, в сети Интернет.

9.4 Оператор обрабатывает персональные данные соискателей в течение срока, необходимого для принятия решения о приеме либо отказе в приеме на работу. В случае отказа в приеме на работу Оператор прекращает обработку персональных данных соискателя в течение 30 дней в соответствии с ч.4 ст.21 ФЗ «О персональных данных». Если соискатель предоставил согласие на внесение его в кадровый резерв, Оператор может продолжить обработку персональных данных в течение срока, указанного в согласии.

9.5 Оператор не обрабатывает специальные категории персональных данных соискателей и биометрические персональные данные соискателей.

9.6 Оператор обрабатывает следующие персональные данные соискателей:

- фамилия, имя, отчество;
- дата рождения;
- образование;
- должность;
- профессия;
- стаж работы;
- номер контактного телефона, адрес электронной почты (по желанию).

10. Обработка персональных данных граждан (пациентов)

10.1 Оператор обрабатывает следующие персональные данные граждан (пациентов) с целью установления медицинского диагноза, оказания медицинских и медико-социальных услуг:
-месяц рождения; дата рождения, место рождения, семейное положение, пол, адрес места жительства, адрес регистрации, СНИЛС, гражданство, данные документа, удостоверяющего личность, данные документа, удостоверяющего личность за пределами Российской Федерации, данные документа, содержащиеся в свидетельстве о рождении, профессия, должность, сведения о состоянии здоровья; анамнез, диагноз, сведения о фактах обращения за медицинской помощью (в целях установления медицинского диагноза; сведения о профпригодности; медицинские изображения; данные об оказании медицинской помощи (вид, условия, сроки, объём, исход, результат обращения); серия и номер выданного листка временной нетрудоспособности; сведения об оказанных медицинских услугах; сведения о медицинских работниках, оказавших медицинскую услугу; сведения о совместном нахождении ребёнка и родителя в стационарных условиях.

11. Сведения об обеспечении безопасности персональных данных

11.1 Оператор назначает ответственного за организацию обработки персональных данных для выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

11.2 Оператор применяет комплекс правовых, организационных и технических мер по обеспечению безопасности персональных данных для обеспечения конфиденциальности персональных данных и их защиты от неправомерных действий:

- обеспечивает неограниченный доступ к Политике, копия которой размещена по адресу нахождения Оператора и на официальном сайте Оператора.
- во исполнение Политики утверждает и приводит в действие документ «Положение об обработке персональных данных» (далее - Положение) и иные локальные акты;
- производит ознакомление работников с положениями законодательства о персональных данных, а также с Политикой и Положением;
- осуществляет допуск работников к персональным данным, обрабатываемым в информационной системе Оператора, а также к их материальным носителям только для выполнения трудовых обязанностей;
- устанавливает правила доступа к персональным данным, обрабатываемым в информационной системе Оператора, а также обеспечивает регистрацию и учет всех действий с ними;
- производит оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ «О персональных данных»;
- производит определение угроз безопасности персональных данных при их обработке в информационной системе Оператора;
- применяет организационные и технические меры и использует средства защиты информации, необходимые для достижения установленного уровня защищенности персональных данных;
- осуществляет обнаружение фактов несанкционированного доступа к персональным данным и принимает меры по реагированию, включая восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- производит оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы Оператора;
- осуществляет внутренний контроль соответствия обработки персональных данных ФЗ «О персональных данных», принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, Политике, Положению и иным локальным актам, включающим контроль за принимаемыми мерами по обеспечению безопасности персональных данных и их уровня защищенности при обработке в информационной системе Оператора.

12.Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

Подсистемы управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

- идентификации и проверки подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн ГБУЗ РК РБ, а также средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн ГБУЗ РК РБ.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;

- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика;
- фиксации во внутренних журналах информации о проходящем открытом и шифрованном IP-трафике;
- идентификации и аутентификации администратора межсетевого экрана при его локальных запросах на доступ;
- регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
- контроля целостности своей программной и информационной части;
- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- регистрации и учета запрашиваемых сервисов прикладного уровня;
- блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС, классом не ниже 4.

Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

Подсистема обнаружения вторжений

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн ГБУЗ РК РБ, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

13. Пользователи ИСПДн

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

В ИСПДн ГБУЗ РК РБ можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратор ИСПДн;
- Администратор безопасности;
- Оператор АРМ;
- Администратор сети;
- Программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положении о разграничении прав доступа к обрабатываемым персональным данным.

Администратор ИСПДн

Администратор ИСПДн, сотрудник ГБУЗ РК РБ, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Администратор безопасности

Администратор безопасности, сотрудник ГБУЗ РК РБ, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

Оператор АРМ

Оператор АРМ, сотрудник ГБУЗ РК РБ, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

Администратор сети

Администратор сети, сотрудник ГБУЗ РК РБ, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

Программист-разработчик ИСПДн

Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники ГБУЗ РК РБ, так и сотрудники сторонних организаций.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

14. Требования к персоналу по обеспечению защиты ПДн

Все сотрудники ГБУЗ РК РБ, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники ГБУЗ РК РБ, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники ГБУЗ РК РБ должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники ГБУЗ РК РБ должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ГБУЗ РК РБ, третьим лицам.

При работе с ПДн в ИСПДн сотрудники ГБУЗ РК РБ обязаны предотвращать возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники ГБУЗ РК РБ должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций;
- Инструкция администратора сети

15. Права субъектов персональных данных

15.1 Субъект персональных данных имеет право:

- на получение персональных данных, относящихся к данному субъекту, и информации, касающейся их обработки;
- на уточнение, блокирование или уничтожение его персональных данных в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- на отзыв данного им согласия на обработку персональных данных;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда в судебном порядке;
- на обжалование действий или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

15.2 Для реализации своих прав и законных интересов субъекты персональных данных имеют право обратиться к Оператору либо направить запрос лично или с помощью представителя. Запрос должен содержать сведения, указанные в ч.3 ст. 14 ФЗ «О персональных данных».

16. Ответственность за нарушение порядка обработки и безопасности персональных данных

16.1 В случае нарушения работником положений законодательства в области персональных данных он может быть привлечен к дисциплинарной, материальной, гражданско-правовой ст 15 и ст. 151 ГК РФ, административной ст.5.39; ч.1-ч.7 ст 13.11, ст 19.7. КоАПП РФ, и уголовной ответственности в порядке, установленном ст. 137, ст.140, ст 272 УК РФ и иными федеральными законами, в соответствии с ч.1 ст.24 ФЗ «О персональных данных» и ст. 90, ст. 192 ТК РФ.

16.2 В случае разглашения работником персональных данных, ставших ему известными в связи с исполнением его трудовых обязанностей, трудовой договор с ним может быть расторгнут в соответствии с подпунктом «в» п.6 ч 1 ст. 81 ТК РФ.

СОГЛАСОВАНО:

Заместитель главного врача по организационно-методической работе

И.И. Тихоненко

«_____» _____

Начальник юридического отдела

О.А. Москвина

«_____» _____

Начальник ОТЗИ ГБУЗ РБ

А.Н. Филимонков

«_____» _____

Начальник оперативного отдела ГБУЗ РБ

В.И.Жирнов

«_____»_____