ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ
«ГОРОДСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА ИМЕНИ В.П. ДЕМИХОВА ДЕПАРТАМЕНТА ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ»

ПРИКАЗ

«20» 01 2025 г. № 50-А

Об утверждении Политики в отношении обработки и защиты персональных данных в ГБУЗ «ГКБ им.В.П.Демихова ДЗМ»

В целях принятия мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» ,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие следующие локальные нормативные акты в области защиты информации:

1.1 Политика в отношении обработки и защиты персональных данных в ГБУЗ «ГКБ им. В.П.Демихова ДЗМ» (Приложение № 1 к настоящему приказу).

1.2. Положение о защите персональных данных, обрабатываемых в информационных системах персональных данных ГБУЗ «ГКБ им.В.П.Демихова ДЗМ» (Приложение № 2 к настоящему приказу)

2. Отделу делопроизводства обеспечить ознакомление с настоящим приказом заместителей главного врача и руководителей подразделений в ГБУЗ «ГКБ имени В.П. Демихова ДЗМ».

3. Начальнику отдела по связям с общественностью Левачевой Т.Н. обеспечить размещение Политики на официальном сайте ГБУЗ «ГКБ им.В.П. Демихова ДЗМ».

4. Считать утратившими силу приказ от 04.07.2024 г. №1080 «Об утверждении Политики в отношении обработки и защиты персональных данных в ГБУЗ «ГКБ имени В.П.Демихова ДЗМ»».

5. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач С.Э.Аракелов

Приложение № 1
к приказу от 10.01 № 50/1

«УТВЕРЖДАЮ»
Главный врач
ГБУЗ «ГКБ им.В.П.Демихова ДЗМ»
_____ С.Э.Аракелов
«10» 01 2019 г.

ПОЛИТИКА
в отношении обработки и защиты персональных данных в ГБУЗ «ГКБ имени В.П. Демихова ДЗМ»

1. Общие положения

1.1. Настоящая Политика в отношении обработки и защиты персональных данных Государственного бюджетного учреждения здравоохранения города Москвы «Городская клиническая больница им. В.П. Демихова Департамента здравоохранения города Москвы» (сокращенное наименование: ГБУЗ «ГКБ имени В.П. Демихова ДЗМ») (далее - Оператор) разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», действует в отношении всех персональных данных, обрабатываемых оператором.

1.2. Политика оператора в отношении обработки персональных данных (далее - Политика) разработана в целях обеспечения защиты прав и свобод субъекта персональных данных при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Основные понятия, используемые в Политике:

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

1.3.2. Обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с

использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение;
- распространение.

1.3.3. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

1.3.4. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

1.3.5. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

1.3.6. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

1.3.7. 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;

1.3.8. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

1.3.9. Оператор персональных данных (оператор) - ГБУЗ «ГКБ им.В.П.Демихова ДЗМ».

1.4. Оператор, получивший доступ к персональным данным, обязан соблюдать конфиденциальность персональных данных - не раскрывать третьим лицам и не

распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

1.5. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

9.1) информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 Федерального закона;

10) иные сведения, предусмотренные Федеральным законом "О персональных данных" или другими федеральными законами.

1.6. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

1.7. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

1.8. Оператор персональных данных вправе:

- отстаивать свои интересы в суде;

- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

- отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;

- использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством.

1.9. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона "О персональных данных".

1.10. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона "О персональных данных".

2. Цели сбора персональных данных

2.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.2. Цели обработки персональных данных происходят в том числе из анализа правовых актов, регламентирующих деятельность оператора, целей фактически осуществляемой оператором деятельности, а также деятельности, которая предусмотрена учредительными документами оператора, и конкретных бизнес-процессов оператора в конкретных информационных системах персональных данных (по структурным подразделениям оператора и их процедурам в отношении определенных категорий субъектов персональных данных).

2.3. К целям обработки персональных данных оператора относятся:

- заключение, исполнение и прекращение гражданско-правовых договоров;

- организация кадрового учета организации, обеспечение соблюдения законов, заключение и исполнение обязательств по трудовым и гражданско-правовым договорам;

- ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, пользовании льготами;

- соблюдения законодательства РФ в сфере здравоохранения;

- организация противодействия терроризму, в том числе путем обеспечения пропускного режима на территорию оператора;

- продвижение товаров и услуг на рынке, в том числе путем размещения информации на сайте больницы;

- исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физических лиц, взносов во внебюджетные фонды и страховых взносов во внебюджетные фонды, пенсионного законодательства при формировании и передаче в ПФР персонифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование;

- заполнение первичной статистической документации в соответствии с трудовым, налоговым законодательством и иными федеральными законами.

3. Правовые основания обработки персональных данных

3.1. Правовым основанием обработки персональных данных являются:

- совокупность правовых актов, во исполнение которых и в соответствии с которыми оператор осуществляет обработку персональных данных: Конституция Российской Федерации; статьи 86-90 Трудового кодекса Российской Федерации, [федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью оператора];

- уставные документы оператора персональных данных;

- договоры, заключаемые между оператором и субъектом персональных данных;

- согласие на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям оператора).

4. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

4.1. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.2. Обработка персональных данных допускается в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом,

для осуществления и выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей;

- обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, трудоустройстве и арбитражных судах;

- обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве;

- обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов внебюджетных фондов, исполнительных органов государственной власти РФ, местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года №210-ФЗ « Об организации предоставления государственных и муниципальных услуг»;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом "О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон "О микрофинансовой деятельности и микрофинансовых организациях", либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона "О персональных данных", при условии обязательного обезличивания персональных данных;

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами ;

4.3. К категориям субъектов персональных данных относятся:

- работники оператора;
- бывшие работники;
- родственники работников;
- соискатели (кандидаты на замещение вакантных должностей);
- контрагенты оператора;
- представители контрагентов;
- клиенты;
- выгодопреобретатели по договорам;
-субъекты персональных данных, предоставившие согласие на трансграничную передачу персональных данных;
- учащиеся;
- студенты;
- законные представители.

4.4. Оператором обрабатываются следующие категории персональных данных:

- фамилия, имя, отчество;
- дата рождения(число, месяц, год);
- место рождения;
- семейное положение;
- социальное положение;
- пол;
- гражданство;
- имущественное положение;
- адрес места жительства и регистрации;
- номера телефонов, адрес электронной почты;
- замещаемая должность;
- сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);
- идентификационный номер налогоплательщика;
- номера расчетного и лицевого счетов, реквизиты банковской карты;
- данные полученного СНИЛС;
- данные документа, удостоверяющего личность;
- данные документа, удостоверяющего личность за пределами территории Российской Федерации;
- отношение к воинской обязанности, сведения о воинском учете
- сведения, содержащиеся в справках о доходах, расходах, об имуществе и обязательствах имущественного характера;
- профессия;

- сведения об образовании;
- сведения о судимости;
- сведения о состоянии здоровья;
- номер расчетного счета;
- фотографии.

5. Порядок и условия обработки персональных данных

5.1. Оператор осуществляет обработку персональных данных - операции, совершаемые с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, распространение, уничтожение персональных данных, .

5.2. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом "О персональных данных".

5.3. Обработка персональных данных оператором ограничивается достижением конкретных, заранее определенных и законных целей. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

5.4. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом , договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.5. При осуществлении хранения персональных данных оператор персональных данных обязан использовать базы данных, находящиеся на территории Российской Федерации, в соответствии с ч. 5 ст. 18 Федерального закона "О персональных данных".

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм

(бланков). При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

5.6. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также ликвидация юридического лица - оператора, изменение законодательства .

5.7. Оператор вправе поручить обработку персональных данных другому лицу на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом "О персональных данных".

Кроме того, оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

5.8. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом "О персональных данных".

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании

персональные данные могут обрабатываться только оператором, которому оно направлено.

5.9. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами. Состав и перечень мер оператор определяет самостоятельно.

5.10. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, указанных в части 2 настоящего пункта:

Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, обязательной государственной геномной регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате.

Оператор не вправе отказывать в обслуживании в случае отказа субъекта персональных данных предоставить биометрические персональные данные и (или) дать согласие на обработку персональных данных, если в соответствии с федеральным законом получение оператором согласия на обработку персональных данных не является обязательным.

5.11. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие 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.

Приложение № 2
к приказу от 30.11 №20.01.11-2

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ГБУЗ «ГКБ им. В.П.Демихова ДЗМ»

1. Назначение и область применения

1.1. Положение об обеспечении безопасности персональных данных (далее – Положение) в информационных системах персональных данных предназначено для организации и проведения мероприятий по обеспечению защиты персональных данных (далее – ПДн) в Государственном бюджетном учреждении здравоохранения города Москвы «Городская клиническая больница имени В.П. Демихова Департамента здравоохранения города Москвы» (далее – ГБУЗ «ГКБ В.П.Демихова ДЗМ») в соответствии с требованиями Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 15 сентября 2008 г. № 687 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных».

1.2. Настоящее Положение определяет порядок организации работ, требования, правила и рекомендации по обеспечению безопасности персональных данных (далее – ПДн) в ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

1.3. Настоящее Положение является внутренним локальным актом ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» по вопросам обеспечения безопасности персональных данных, обрабатываемых в ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ». Требования Положения обязательны для выполнения всеми работниками ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ», которые допущены к обработке персональных данных и реализуют мероприятия по защите персональных данных.

2. Общие положения

2.1. Целью защиты ПДн является предотвращение возможной утечки информации и (или) несанкционированного и непреднамеренного изменения или разрушения ПДн.

2.2. Защита ПДн достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа, программно-математических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

2.3. Все сотрудники ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ», обрабатывающие ПДн и обеспечивающие защиту ПДн, должны быть ознакомлены с настоящим Положением под подпись.

3. Персональные данные, подлежащие защите

3.1. Персональные данные, подлежащие защите в ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ», обрабатываются без использования средств автоматизации, а также с использованием средств автоматизации в ИСПДн.

3.2. Проверка соответствия состава обрабатываемых персональных данных осуществляется ежегодно в рамках проведения уполномоченными сотрудниками ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» мероприятий по контролю состояния защиты персональных данных в ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ». Изменения, дополнения перечня персональных данных, обрабатываемых в ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ», осуществляются ежегодно на основании информации, предоставляемой руководителями подразделений, в которых осуществляется обработка персональных данных.

4. Организационная система обеспечения безопасности персональных данных

4.1. В состав организационной системы обеспечения безопасности ПДн ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» входят:

– Главный врач ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ»;

– Ответственные за организацию обработки и обеспечение безопасности персональных данных, назначаемые приказом главного врача ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» из числа должностных лиц руководящего состава ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ»;

– Администратор безопасности ИСПДн (далее - Администратор ИБ), назначаемый приказом главного врача ГБУЗ «ГКБ им. В.П. ДЕМИХОВА

ДЗМ» из числа сотрудников подразделения, выполняющего функции по защите информации;

– Администратор ИСПДн, назначаемый приказом главного врача ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» из числа сотрудников подразделения, выполняющего функции по обеспечению работоспособности ИСПДн;

– Руководители подразделений ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ», в которых осуществляется обработка ПДн.

4.2. Общее руководство организацией работ по защите ПДн осуществляет главный врач ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

4.3. Ответственные за организацию обработки и обеспечение безопасности персональных данных получает указания непосредственно от главного врача ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» и подотчетны ему.

4.4. Ответственные за организацию обработки и обеспечение безопасности персональных данных, в рамках обеспечения безопасности ПДн выполняют следующие функции:

– организует процессы разработки, утверждения и корректировки локальных правовых актов ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» по обеспечению безопасности ПДн;

– доводит до сведения сотрудников ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– организует внутренний контроль за соблюдением сотрудниками ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

4.5. Ответственные за организацию обработки и обеспечение безопасности персональных данных также осуществляют организацию работ по созданию системы защиты ПДн (далее – СЗПДн) и разработке организационно-распорядительных документов (далее – ОРД), регламентирующих вопросы обеспечения безопасности ПДн.

4.6. Администратор ИБ выполняет следующие функции:

– согласовывает изменения списка пользователей ИСПДн;

– осуществляет контроль настроек средств защиты информации в соответствии с изменениями в списке пользователей ИСПДн;

– осуществляет взаимодействие со структурными подразделениями ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ», в том числе обеспечивает и обобщает предложения от подразделений по совершенствованию и реализации мероприятий по обеспечению безопасности ПДн в ИСПДн ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ»;

– контролирует деятельность структурных подразделений ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» по выполнению ими установленных требований обеспечения безопасности ПДн в ИСПДн ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ»;

– организует расследования по фактам разглашения или утечки персональных данных в ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

4.7. Права и обязанности администратора ИСПДН определены регламентами управления (администрирования) системы обеспечения ИБ ИС СМУ, управления конфигурацией ИС СМУ и другими документами, регламентирующими работу ИС.

4.8. Администратор ИСПДн выполняет следующие функции:

– вносит изменения списка пользователей ИСПДн;

– осуществляет системное администрирование серверов, сетевого оборудования, администрирование прикладных систем ИСПДн, рабочих станций ИСПДн;

– осуществляет резервное копирование защищаемых информационных ресурсов;

– контролирует деятельность структурных подразделений ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» по выполнению ими установленных правил работы в ИСПДн ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

4.9 Права и обязанности администратора ИБ определены в «Инструкции администратора ИБ ИС СМУ».

4.10 Руководители подразделений ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ», сотрудникам которых предоставлен доступ к ПДн:

– формируют заявки на допуск пользователей к обработке ПДн в ИСПДн;

– обеспечивают выполнение мероприятий по защите ПДн в подразделениях ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ»;

– готовят предложения в перечень персональных данных, в список сотрудников, допущенных в помещения, где ведется обработка ПДн и в список сотрудников, допущенных к работе в ИСПДн, предназначенных для выполнения функций подразделения.

4.11 Сотрудники, которым предоставлен доступ к обработке ПДн без использования средств автоматизации, реализуют организационные меры по обеспечению сохранности носителей ПДн и выполнению процедур по соблюдению требований законодательства.

4.12 Пользователи ИСПДн ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» реализуют требования безопасности информации, принятые для ИСПДн, исполняют установленные режимы защиты ПДн, обеспечивают строгое исполнение предписанных правил работы в ИСПДн. Права и обязанности пользователей ИСПДн определены в «Инструкции пользователя ИС СМУ».

5. Защита персональных данных при обработке без использования средств автоматизации

5.1 Требования к обеспечению безопасности персональных данных при их обработке без использования средств автоматизации установлены Постановлением Правительства РФ от 15.09.2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5.2 Защита ПДн, обрабатываемых без использования средств автоматизации, обеспечивается выполнением следующих мероприятий:

– определением мест хранения персональных данных (материальных носителей) и перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

– обеспечением раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

– соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним. Бумажные носители ПДн подлежат уничтожению по достижении целей обработки и/или в случае истечения их сроков хранения носителей ПДн. Уничтожение носителей осуществляется по Акту. Бумажные носители ПДн постоянного срока хранения (свыше 5 лет) передаются в архив ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

6. Защита персональных данных при обработке в информационных системах персональных данных

6.1 Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

1) Определение требуемого уровня защищенности ИСПДн ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

2) Определение угроз безопасности персональных данных при их обработке в ИСПДн, формирование на их основе модели угроз.

3) Разработка модели нарушителя.

4) Разработка на основе модели угроз и модели нарушителя системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего уровня защищенности информационных систем.

5) Применение прошедших в установленном порядку процедуру оценки соответствия средств защиты информации.

6) Описание системы защиты персональных данных.

7) Установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией.

8) Обучение лиц, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними.

9) Оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

10) Установление 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.

11) Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, машинных носителей персональных данных.

12) Учет лиц, допущенных к работе с персональными данными в информационной системе.

13) Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных, включая контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

14) Разбирательство и составление заключений по фактам несоблюдения условий хранения машинных носителей персональных данных, некорректного использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям,

приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

15) Принятие мер в случае обнаружения фактов несанкционированного доступа к персональным данным.

16) Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

6.2 Определение уровня защищенности ИСПДн и моделирование угроз безопасности ПДн.

1) Определение уровня защищенности ИСПДн проводится в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» (утвержденными Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119).

2) Определение уровня защищенности ИСПДн проводит специальная Комиссия, состав которой утверждается приказом главного врача ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

3) Результаты работы Комиссии утверждаются Актом установления уровня защищенности ИСПДн.

4) Уровень защищенности ИСПДн может быть пересмотрен:

– по решению Комиссии по определению уровня защищенности информационных систем персональных данных при изменении характеристик ИСПДн;

– по решению Комиссии по определению уровня защищенности информационных систем персональных данных, исходя из результатов проведенных мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

5) Уточнение и пересмотр уровня защищенности ИСПДн осуществляется в случае изменения:

– состава обрабатываемых ПДн в ИСПДн (изменении категории ПДн);

– количества обрабатываемых ПДн;

– типа актуальных угроз безопасности ПДн (угрозы наличия и использования недекларированных возможностей в системном или прикладном ПО).

6) Все имеющиеся и вводимые в эксплуатацию ИСПДн вносятся в перечень ИСПДн ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

7) Выявление угроз безопасности ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе метода экспертных оценок, в том числе путем опроса специалистов по информационным технологиям, персонала ИСПДн, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса могут составляться специальные опросные листы.

8) Уточнение и пересмотр угроз безопасности ПДн при их обработке в ИСПДн осуществляется вне зависимости от проведения плановых проверок состояния защиты ПДн в случаях:

– изменения технологических процессов обработки ПДн;

– изменения состава средств защиты информации в ИСПДн;

– изменения характеристик ИСПДн, влияющих на уровень защищенности (наличие подключений к сетям общего пользования, тип ИСПДн и т.д.).

9) При необходимости применения (в случае передачи ПДн по незащищенным каналам связи) средств криптографической защиты информации для ИСПДн разрабатывается Модель нарушителя безопасности персональных данных на основе «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных» ФСБ России. На основе такой модели нарушителя для ИСПДн определяется уровень криптографической защиты ПДн, которому должны соответствовать применяемые средства криптографической защиты.

6.3 Требования к обеспечению безопасности ПДн при их обработке в ИСПДн.

1) Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных (СЗПДн), включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

2) Требования к СЗПДн разрабатываются на основе модели угроз и модели нарушителя и должны обеспечивать нейтрализацию предполагаемых актуальных угроз, выявленных по результатам моделирования. Требования формируются на основании методов и способов защиты информации для соответствующего класса информационных систем, задаваемых требованиями нормативных документов по защите ПДн ФСТЭК России и ФСБ России.

3) Методы и способы защиты персональных данных включают в себя:

– реализацию разрешительной системы допуска пользователей к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

– разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– регистрацию действий пользователей, контроль несанкционированного доступа и действий пользователей, посторонних лиц;

– учет и хранение съемных носителей информации, их обращение, исключающее хищение, подмену и уничтожение;

– резервирование технических средств, дублирование массивов и носителей информации;

– использование сертифицированных средств защиты информации;

– использование защищенных каналов связи;

– размещение технических средств, позволяющих осуществлять обработку персональных данных, только в пределах охраняемой территории (рабочие станции, серверы, коммутационное оборудование, сетевые принтеры);

– организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку персональных данных;

– предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) с использованием средств антивирусной защиты.

6.4 Разрешительная система допуска пользователей к информационным ресурсам.

1) Разграничение доступа к информационным ресурсам, содержащим ПДн, должно осуществляться в соответствии с «Положением о разрешительной системе доступа в ИСПДн», на основании должностных обязанностей сотрудников, допущенных к работе с персональными данными в ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ». Список сотрудников ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ», доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных, необходим для выполнения служебных обязанностей, утверждается приказом главного врача ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

2) Допуск сотрудника к информационным ресурсам ИСПДн должен оформляться в виде заявки на регистрацию и/или предоставление доступа к сетевым ресурсам от руководителей структурных подразделений ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ», согласованной с руководителем подразделения ИТ и Администратором безопасности ИСПДн ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

3) Согласованная заявка на допуск сотрудника к информационным ресурсам ИСПДн передается на исполнение в подразделение ИТ ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ». Заявка должна храниться в подразделении ИТ ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» в течение всего срока эксплуатации ИСПДн.

4) Проводится регулярная проверка соответствия пользователей ИСПДн, определенных в матрице доступа к ИСПДн, с имеющимися заявками на предоставление доступа сотрудников ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» к ИСПДн.

6.5 Регистрация действий пользователей.

1) Регистрация действий пользователей должна осуществляться средствами системного программного обеспечения и СЗИ ИСПДн.

2) Подлежат обязательной регистрации следующие операции, осуществляемые в ИСПДн:

– регистрация входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова;

– регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;

– регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

– регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа.

6.6 Обеспечение безопасности при хранении носителей информации ПДн.

1) Подлежат учету следующие защищаемые носители ПДн:

– накопители на жестких магнитных дисках, установленные в серверы ИСПДн;

– накопители на жестких магнитных дисках, установленные в АРМ, на которых предусмотрено хранение ПДн;

– накопители для хранения резервных копий;

– внешние носители ПД (дискеты, компакт-диски, flash-накопители), на которых технологией обработки ПДн разрешается хранение или передача ПДн.

2) Учет защищаемых носителей информации должен осуществляться в Журналах учета электронных носителей ПДн в соответствии с «Положением о порядке учета, хранения и уничтожения машинных носителей ПДн».

3) Обязанность по ведению учета внешних носителей ПДн (дискет, компакт-дисков, flash-дисков, на которые осуществляется кратковременное хранение ПДн и/или передача их во внешние организации) возлагается на Администратора безопасности ИСПДн ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

4) В случае смены владельца или назначения, списания и выведения из эксплуатации защищаемых носителей информации необходимо обеспечить уничтожение ПДн с носителей. Уничтожение информации с носителей информации должно осуществляться путем многократной записи информации на носители и/или путем физического уничтожения носителя.

5) По факту уничтожения носителя ПДн должен составляться соответствующий Акт.

6.7 Резервирование технических средств, дублирование массивов и носителей информации.

1) Обеспечение целостности и доступности ПДн, программных и аппаратных средств ИСПДн, а также средств защиты, при их случайной или намеренной модификации, должно осуществляться с помощью резервного копирования (дублирования массивов и носителей информации) обрабатываемых данных, резервирования элементов ИСПДн.

2) Для обеспечения целостности ИСПДн должны выполняться следующие мероприятия по резервированию:

– резервные копии информационных ресурсов, содержащих ПДн, должны храниться в специально выделенном месте, территориально отдаленном от места обработки самой информации;

– для обеспечения сохранности резервных копий должен быть применён комплекс организационных и физических мер защиты от НСД;

– носители, на которые осуществляется резервное копирование, должны регулярно проверяться на отсутствие механических повреждений, сбоев логической структуры, файловой системы;

– должны проводиться регулярные проверки процедур восстановления данных.

6.8 Использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия.

1) При защите ПДн используются СЗИ, сертифицированные в системах сертификации Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации в пределах их полномочий.

2) При использовании средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия (сертификацию), должны выполняться следующие мероприятия:

– установка и ввод в эксплуатацию средств защиты информации осуществляется в соответствии с эксплуатационной и технической документацией сотрудниками центра информационных технологий ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ»;

– проведение обучения работников ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ», использующих средства защиты, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним.

– контроль Администратором ИБ соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– проведение Администратором ИБ разбирательств и составление заключений по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению целостности, конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

6.9 Использование защищенных каналов связи.

1) При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) основными методами и способами защиты информации от несанкционированного доступа являются:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

– обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

– анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

– защита информации при ее передаче по каналам связи;

– использование средств антивирусной защиты;

– централизованное управление системой защиты персональных данных информационной системы.

2) Для обеспечения безопасности персональных данных при удаленном доступе к информационной системе через информационно-телекоммуникационную сеть международного информационного обмена дополнительно должны применяться следующие основные методы и способы защиты информации от несанкционированного доступа:

– проверка подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети международного информационного обмена данных;

– управление доступом к защищаемым персональным данным информационной сети.

3) Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных информационных систем через информационно-телекоммуникационную сеть международного информационного обмена должны применяться следующие основные методы и способы защиты информации от несанкционированного доступа:

– создание канала связи, обеспечивающего защиту передаваемой информации;

– осуществление аутентификации взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных.

6.10 Физическая защита помещений и технических средств.

1) Размещение ИСПДн и охрана помещений, в которых ведется работа с персональными данными, должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

2) Выполнение требований по исключению возможности неконтролируемого проникновения или пребывания в помещениях ИСПДн посторонних лиц реализуется осуществлением организационных и технических мер по созданию контролируемой зоны (КЗ) ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

3) Границами КЗ могут являться:

– периметр охраняемой территории ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ»;

– ограждающие конструкции охраняемого здания;

– стены помещений ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

4) В состав КЗ должны входить

– помещения, в которых размещены рабочие станции, серверы, сетевое оборудование, входящие в состав ИСПДн;

– помещения, в которых проходят кабельные линии связи ИСПДн;

– помещения, в которых хранятся бумажные носители ПДн (архивы, помещения сотрудников ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ»).

5) Размещение технических средств, обрабатывающих ПДн, должно осуществляться с учетом требования минимизации доступа в рабочие помещения лиц, не связанных с обработкой ПДн и обслуживанием оборудования.

6) Доступ посторонних лиц (посетителей, работников обслуживающих организаций) в контролируемую зону в рабочее время осуществляется только в сопровождении работников ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

7) Размещение устройств отображения и печати информации, используемых в составе ИСПДн, должно осуществляться с учетом максимального затруднения визуального просмотра информации посторонними лицами.

8) Серверы и коммуникационное оборудование ИСПДн должны располагаться в отдельном помещении или в металлических шкафах с прочной запираемой дверью. Ключи от дверей помещений и шкафов должны быть только у лиц, имеющих право доступа в них.

9) В нерабочее время доступ в контролируемую зону должен быть исключен следующими мерами:

– заключением договора с арендодателем (охранным предприятием), обязательными условиями которого являются следующие обязанности арендодателя (охранного предприятия):

– организация и обеспечение контроля доступа в арендуемые помещения работников и посетителей в рабочее время.

– организация и обеспечение охраны помещений в нерабочее время, а также в выходные и праздничные дни.

– не допускать проникновения и пребывания посторонних лиц в помещениях в нерабочее время, а также в выходные и праздничные дни. При необходимости использования помещений в указанное время, допуск в помещения осуществляется по письменной заявке ответственным лицом.

– в случае отсутствия возможности заключения договора с арендодателем (охранным предприятием) для реализации мер по охране контролируемой зоны в нерабочее время необходимо выполнять следующие требования:

– на всех остекленных проемах первого и последнего этажа должны быть установлены металлические решетки или ставни с запорами;

– двери в помещения контролируемой зоны должны быть с надежными замками;

– хранение ключей осуществляется назначенным приказом главного врача ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» ответственным лицом с выдачей под роспись сотрудникам ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» в случае необходимости.

6.11 Использование средств антивирусной защиты.

1) Средства антивирусной защиты предназначены для реализации следующих функций:

– антивирусное сканирование;

– блокирование вредоносных программ;

– автоматизированное обновление антивирусных баз;

– ограничение прав пользователя на изменение настроек антивирусного программного обеспечения;

– автоматический запуск сразу после загрузки операционной системы.

2) Подсистема антивирусной защиты реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

3) Обо всех случаях сбоев антивирусного программного обеспечения (появления сообщений об ошибках) пользователь должен немедленно уведомлять Администратора ИБ.

6.12 Порядок разработки, ввода в действие и эксплуатации СЗПДн

1) Требования по защите ПДн для каждой ИСПДн должны формироваться в виде Технического задания на создание СЗПДн в ИСПДн на этапе разработки (модернизации) ИСПДн.

2) Требования должны формироваться на основании положений руководящих документов ФСТЭК России и ФСБ России.

3) Для вновь создаваемых ИСПДн, а также для функционирующих ИСПДн, не включающих в себя СЗПДн проводятся следующие мероприятия:

– обследование ИСПДн и разработка технического (частного технического) задания на создание СЗПДн;

– проектирование и реализация ИСПДн и СЗПДн в её составе;

– ввод в действие СЗПДн, включающее опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

4) Для функционирующих ИСПДн, включающих в себя СЗПДн, доработка (модернизация) СЗПДн должна проводиться в случае, если:

– изменился состав обрабатываемых ПДн;

– изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ЛВС ИСПДн) или

технологический процесс обработки ПДн, вследствие которого произошли изменения в структуре ИСПДн;

– изменился состав угроз безопасности ПДн в ИСПДн;

– изменился класс ИСПДн.

6.13 Порядок оценки эффективности принимаемых мер по обеспечению безопасности ПДн в период эксплуатации ИСПДн.

1) Оценка эффективности принимаемых мер в ИСПДн выполняется в соответствии с внутренними проверками, а также на основании доказательств, полученных с участием привлеченных организаций (внешний аудит), имеющих необходимые лицензии ФСТЭК РФ и ФСБ РФ.

7. Требования к персоналу по обеспечению безопасности персональных данных

7.1. При вступлении в должность нового сотрудника непосредственный руководитель структурного подразделения ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ», в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими порядок обработки и обеспечения защиты ПДн. Администратор ИБ обучает навыкам выполнения процедур, необходимых для работы в ИСПДн ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» и выполнения требований по защите ПДн в ИСПДн.

7.2. Сотрудники ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» должны соблюдать установленные организационно-распорядительными документами требования по режиму обработки персональных данных, учету, хранению, передаче носителей информации и обеспечению безопасности ПДн.

7.3. Сотрудники ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» должны быть проинформированы об ответственности за нарушение требований по обеспечению безопасности ПДн на момент заключения трудового договора с ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» специалистами подразделения по работе с персоналом (кадрами).

8. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных

8.1. Целью контроля состояния защиты является своевременное выявление и предотвращение утечки информации.

8.2. Контроль состояния защиты ПДн в ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ» должен осуществляться ежегодно, в соответствии с утвержденным Планом внутренних проверок состояния защиты персональных данных.

8.3. Проведение контроля состояния защиты включает в себя мероприя-

тия по оценке:

– соблюдения требований руководящих и нормативно-методических документов по защите ПДн;

– работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

– знания и выполнения персоналом своих функциональных обязанностей в части защиты ПДн.

8.4. Проверка проводится дополнительно при изменении состава технических средств и систем, условий обработки информации, содержащей ПДн.

9. Принятие мер в случае обнаружения фактов нарушения требований (несанкционированного доступа к ПДн), разбирательство и составление заключений по фактам нарушения требований безопасности

9.1. Лицо, обнаружившее факт нарушения требований, незамедлительно уведомляет Администратора ИБ о факте нарушения.

9.2. В случаях обнаружения нарушений при обработке ПДн в ИСПДн необходимо:

– немедленно прекратить обработку ПДн в ИСПДн, где обнаружены нарушения и принять меры к их устранению;

– организовать расследование причин и условий появления нарушений с целью недопущения их в дальнейшем;

– разработать план мероприятий по устранению нарушений.

9.3. Возобновление работ разрешается только после выполнения мероприятий по устранению нарушений и проверки достаточности и эффективности принятых мер.

9.4. Порядок выполнения мероприятий, указанных в п. 9.2. определяется отдельными локальными нормативными актами ГБУЗ «ГКБ им. В.П. ДЕМИОВА ДЗМ».

10. Порядок внесения изменений

10.1. Настоящее Положение пересматривается раз в три года и в случае изменения законодательства в области защиты ПДн.

10.2. Все изменения и дополнения в настоящее Положение вносятся приказом главного врача ГБУЗ «ГКБ им. В.П. ДЕМИХОВА ДЗМ».

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ изменения	Номера страниц				Всего страниц	Дата	Подпись лица, вносившего изменения
	измененных	замененных	аннулированных	новых			