ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ
«ДИАГНОСТИЧЕСКИЙ КЛИНИЧЕСКИЙ ЦЕНТР № 1
ДЕПАРТАМЕНТА ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ»
117485, г. Москвы, ул. Миклухо-Маклая, д. 29, корп. 2; тел. (495) 336-67-55; факс (495) 336-69-22; e-mail: kdc1@zdrav.mos.ru

ПРИКАЗ № 530

г. Москва от 15 сентября 2021 г.

"Об утверждении локальных нормативных актов по организации обработки и обеспечению безопасности персональных данных (далее – Положения) в ГБУЗ "ДКЦ № 1 ДЗМ»

В целях реализации требований Федерального закона Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных», обеспечения защиты прав и свобод граждан при обработке их персональных данных, в том числе неприкосновенности частной жизни,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие следующие локальные нормативные акты по организации обработки и обеспечению безопасности персональных данных (далее – Положения) в ГБУЗ "ДКЦ № 1 ДЗМ»:

- ПОЛИТИКА ГБУЗ «ДКЦ № 1 ДЗМ» в отношении обработки персональных данных
- Правила обработки персональных данных субъектов персональных данных в ГБУЗ «ДКЦ № 1 ДЗМ»
- ПРАВИЛА рассмотрения ГБУЗ «ДКЦ № 1 ДЗМ» запросов субъектов персональных данных или их представителей
- ПРАВИЛА осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
- ПРАВИЛА работы с обезличенными данными в ГБУЗ «ДКЦ № 1 ДЗМ»
- ПЕРЕЧЕНЬ персональных данных, обрабатываемых в ГБУЗ «ДКЦ № 1 ДЗМ»
- ПЕРЕЧЕНЬ должностей работников ГБУЗ «ДКЦ № 1 ДЗМ, замещение которых предусматривает осуществление обработки персональных данных
- ПЕРЕЧЕНЬ мест хранения материальных носителей персональных данных, обрабатываемых без использования средств автоматизации
- ОБЯЗАТЕЛЬСТВО о неразглашении и обеспечении безопасности персональных данных
- ОБЯЗАТЕЛЬСТВО государственного гражданского служащего, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора
- ФОРМА разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные
- ПОРЯДОК Ответственность за нарушение порядка обработки и обеспечения безопасности персональных данных
- ПОЛОЖЕНИЕ о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
- СОГЛАСИЕ на передачу персональных данных

2. Назначить ответственным за применение и соблюдение всех локальных нормативных актов начальника информационно-аналитического отдела Пархоменко Михаила Генриховича
3. Довести содержание настоящего приказа до сведения руководителей структурных подразделений ГБУЗ "ДКЦ № 1 ДЗМ"
4. Контроль исполнения настоящего приказа оставляю за собой.

Приложение:

1. Локальные нормативные акты по обеспечению безопасности персональных данных в ГБУЗ "ДКЦ № 1 ДЗМ».

Главный врач **В.П. Сидорова**

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

ПОЛИТИКА

Государственного бюджетного учреждение здравоохранения города Москвы «Диагностический клинический центр № 1 Департамента здравоохранения города Москвы» (ГБУЗ «ДКЦ № 1 ДЗМ») в отношении обработки персональных данных

1 Общие положения

1.1 Политика ГБУЗ «ДКЦ № 1 ДЗМ» в отношении обработки и защиты персональных данных (далее – Политика) определяет основные принципы обработки персональных данных субъектов персональных данных (далее – персональные данные) и защиты прав субъектов персональных данных, персональные данные которых обрабатываются ГБУЗ «ДКЦ № 1 ДЗМ».

1.2 Политика разработана в соответствии с требованиями законодательства Российской Федерации в области персональных данных, в том числе Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон «О персональных данных»), а также иными нормативными правовыми актами Российской Федерации и города Москвы, регулирующими обработку и защиту персональных данных.

1.3 В настоящей Политике под оператором информационной системы понимается юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Остальные термины и определения, используемые в настоящей Политике, соответствуют терминологии, принятой в статье 3 Закона «О персональных данных».

2 Субъекты персональных данных, правовые основания и цели обработки персональных данных

Правовым основанием обработки персональных данных субъектов персональных данных ГБУЗ «ДКЦ № 1 ДЗМ» является исполнение возложенных на ГБУЗ «ДКЦ № 1 ДЗМ» законодательством Российской Федерации функций, полномочий и обязанностей в соответствии с федеральными законами, в том числе, но не ограничиваясь: *К применимому законодательству относятся: Налоговый кодекс Российской Федерации, Гражданский кодекс Российской Федерации, Трудовой кодекс Российской Федерации, Федеральный закон от 09.02.2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федеральный закон от 02.05.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральный закон от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федеральный закон от 16 июля 1999 г. № 165-ФЗ «Об основах обязательного социального страхования», Федеральный закон от 15 декабря 2001 г. № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации», Федеральный закон от 29 декабря 2006 г. № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством», Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральный закон от 01.04.1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», Федеральный закон от 28.12.2013 г. № 400-ФЗ «О страховых пенсиях», Федеральный закон от 15.12.2001 г. № 166-ФЗ «О государственном пенсионном обеспечении в Российской Федерации», Федеральный закон от 26.02.1997 г. № 31-ФЗ «О мобилизационной подготовке и мобилизации в Российской Федерации», Федеральный закон от 06.12.2011 г. № 402-ФЗ «О бухгалтерском учете», Постановление Правительства от 27 ноября 2006 г. № 719 «Об утверждении Положения о воинском учете», закон г. Москвы от 26.01.2005 г. № 3 «О государственной гражданской службе города Москвы» и др.*

2.1 Субъектами персональных данных, данные которых обрабатываются в ГБУЗ «ДКЦ № 1 ДЗМ» являются:

– *представители организаций – участников закупок, проводимых Организацией в соответствии с требованиями федерального закона от 05 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – участники закупок);*

– *представители контрагентов;*

– *физические лица, обратившиеся в Организацию с жалобой, предложением, заявлением или направившие запрос о предоставлении информации о деятельности Организации, ее подведомственных учреждений и предприятий;*

– *физические лица, предоставившие свои персональные в рамках исполнения Организацией своих полномочий.*

2.2 Обработка персональных данных субъектов ПДн в ГБУЗ «ДКЦ № 1 ДЗМ» осуществляется в целях:

2.3 *обеспечения соблюдения федеральных законов и иных нормативных актов Российской Федерации и города Москвы, регулирующих вопросы ведения бухгалтерского, налогового и воинского учета, кадровой работы при прохождении гражданами государственной гражданской службы города Москвы в Организации;*

– *обеспечение соблюдения федеральных законов и иных нормативных правовых актов Российской Федерации, регулирующих вопросы участия граждан в конкурсах на включение в кадровый резерв и замещение вакантных должностей государственной гражданской службы города Москвы в Организации;*

– *оформление доверенностей работникам;*

– *проведение закупок в соответствии с требованиями Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;*

– *заключение и исполнение государственных контрактов с контрагентами;*

– *обеспечение соблюдения федеральных законов и иных нормативных, правовых актов, регламентирующих правоотношения в сфере рассмотрения обращений физических и юридических лиц, обеспечение доступа к информации о деятельности государственных органов;*

– *предоставление государственных или муниципальных услуг и осуществления государственных или муниципальных функций.*

3 Принципы и правила обработки персональных данных

3.1 При обработке персональных данных ГБУЗ «ДКЦ № 1 ДЗМ» соблюдаются следующие принципы:

– обработка персональных данных осуществляется на законной и справедливой основе;

– обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

– не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

– не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только персональные данные, которые отвечают целям их обработки;

– содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки;

– обрабатываемые персональные данные не являются избыточными по отношению к заявленным целях их обработки;

– при обработке персональных данных обеспечивается точность персональных данных, их достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных;

– принимаются необходимые меры по удалению или уточнению неполных или неточных персональных данных;

– хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством Российской Федерации и города Москвы;

– обрабатываемые персональные данные уничтожаются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

3.2 В ГБУЗ «ДКЦ № 1 ДЗМ» осуществляется как автоматизированная обработка персональных данных, так и неавтоматизированная обработка персональных данных (обработка персональных данных без использования средств автоматизации; обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого субъекта персональных данных осуществляются при непосредственном участии человека). Совокупность операций обработки персональных данных в ГБУЗ «ДКЦ № 1 ДЗМ» включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, распространение, доступ), блокирование, удаление, уничтожение персональных данных.

3.3 При сборе персональных данных ГБУЗ «ДКЦ № 1 ДЗМ» обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных с использованием баз данных, находящихся на территории Российской Федерации.

3.4 Перечень обрабатываемых ГБУЗ «ДКЦ № 1 ДЗМ» персональных данных утверждается распоряжением главного врача ГБУЗ «ДКЦ № 1 ДЗМ».

3.5 Допускается обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

3.6 ГБУЗ «ДКЦ № 1 ДЗМ» осуществляет передачу персональных данных третьим лицам в соответствии с требованиями законодательства Российской Федерации в области обработки и защиты персональных данных.

3.7 ГБУЗ «ДКЦ № 1 ДЗМ» в ходе своей деятельности вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного контракта, либо путем принятия государственным органом соответствующего акта. При этом обязательным условием предоставления и/или поручения обработки персональных данных другому лицу является обязанность сторон по соблюдению конфиденциальности и обеспечению безопасности персональных данных при их обработке.

3.8 В случаях, когда ГБУЗ «ДКЦ № 1 ДЗМ» поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет ГБУЗ «ДКЦ № 1 ДЗМ». Лицо, осуществляющее обработку персональных данных по поручению Департамента, несет ответственность перед ГБУЗ «ДКЦ № 1 ДЗМ».

3.9 Прекращение обработки персональных данных осуществляется при прекращении деятельности ГБУЗ «ДКЦ № 1 ДЗМ» (ликвидация или реорганизация).

4 Сроки обработки персональных данных

4.1 Сроки обработки (в т.ч. хранения) персональных данных, обрабатываемых ГБУЗ «ДКЦ № 1 ДЗМ», определяются исходя из целей обработки персональных данных и в соответствии с требованиями федеральных законов Российской Федерации.

5 Меры обеспечения безопасности персональных данных, принимаемые ГБУЗ «ДКЦ № 1 ДЗМ»

5.1 ГБУЗ «ДКЦ № 1 ДЗМ» принимает или обеспечивает принятие необходимых и достаточных правовых, организационных и технических мер 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.

5.2 К таким мерам в ГБУЗ «ДКЦ № 1 ДЗМ» относятся:

– назначение лица, ответственного за организацию обработки персональных данных;

– издание локальных актов по вопросам обработки персональных данных и локальных актов, устанавливающих процедуры, направленные на предотвращение и выявления нарушений законодательства Российской Федерации в области обработки и защиты персональных данных, устранение последствий таких нарушений;

– применение или обеспечение применения правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со ст.19 Закона «О персональных данных»;

– осуществление внутреннего контроля соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, требованиям к защите персональных данных, внутренним документам ГБУЗ «ДКЦ № 1 ДЗМ» в области обработки и защиты персональных данных;

– оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых ГБУЗ «ДКЦ № 1 ДЗМ» мер (или мер, обеспечение принятия которых осуществляется ГБУЗ «ДКЦ № 1 ДЗМ»), направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

– ознакомление работников ГБУЗ «ДКЦ № 1 ДЗМ» с положениями законодательства Российской Федерации о персональных данных, внутренними документами ГБУЗ «ДКЦ № 1 ДЗМ» по вопросам обработки персональных данных, требованиями к защите персональных данных.

6 Взаимодействие с субъектами персональных данных

6.1 Права субъектов персональных данных определяются статьями 14-17 Закона «О персональных данных».

6.2 Для осуществления своих прав субъект персональных данных может лично или через законного представителя обратиться в ГБУЗ «ДКЦ № 1 ДЗМ» путем направления письменного запроса по адресу: 117485, г. Москва, ул. Миклухо-Маклая, д. 29, корп. 2.

6.3 Запрос должен содержать:

– номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;

– сведения о дате выдачи указанного документа и выдавшем его органе;

– сведения, подтверждающие участие субъекта персональных данных в отношениях с ГБУЗ «ДКЦ № 1 ДЗМ» (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных ГБУЗ «ДКЦ № 1 ДЗМ» ;

– подпись субъекта персональных данных или его представителя.

6.4 Порядок рассмотрения запросов осуществляется ГБУЗ «ДКЦ № 1 ДЗМ» в порядке, установленном Законом «О персональных данных».

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

Правила обработки персональных данных субъектов персональных данных в ГБУЗ «ДКЦ № 1 ДЗМ», устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований

1. Общие положения

1.1. Настоящие правила обработки персональных данных субъектов персональных данных в ГБУЗ «ДКЦ № 1 ДЗМ»] (далее – Правила) разработаны в целях:

- обеспечения защиты прав и свобод субъектов персональных данных при обработке персональных данных в ГБУЗ «ДКЦ № 1 ДЗМ»;
- установления процедур, направленных на выявление и предотвращение нарушений законодательства Российской Федерации о персональных данных, иных правовых актов Российской Федерации, города Москвы (далее – законодательство в сфере персональных данных), внутренних документов ГБУЗ «ДКЦ № 1 ДЗМ» по вопросам обработки и защиты персональных данных;
- определения целей обработки ГБУЗ «ДКЦ № 1 ДЗМ» персональных данных в установленной сфере деятельности, включая содержание обрабатываемых персональных данных, категории субъектов персональных данных, данные которых обрабатываются, сроки обработки (в т.ч. хранения) обрабатываемых персональных данных, а также порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований;
- установления ответственности работников ГБУЗ «ДКЦ № 1 ДЗМ», имеющих доступ к персональных данных субъектов персональных данных (далее - ПДн), за невыполнение требований норм, регулирующих обработку ПДн, установленных законодательством Российской Федерации, настоящим документом и иными внутренними документами ГБУЗ «ДКЦ № 1 ДЗМ».

1.2. Настоящие Правила разработаны в соответствии с законодательством Российской Федерации в области обработки и защиты ПДн и нормативными правовыми актами города Москвы.

1.3. Действие настоящих Правил не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов, а также при обработке ПДн, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.4. Из числа работников ГБУЗ «ДКЦ № 1 ДЗМ» определяются лица, осуществляющие обработку ПДн в ГБУЗ «ДКЦ № 1 ДЗМ» и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение требований в области обработки и защиты ПДн.

2. Основные понятия

В настоящих Правилах используются следующие основные понятия и определения:

2.1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.2. Безопасность ПДн – комплекс мер, соответствующих требованиям законодательства в сфере защиты ПДн, направленных на обеспечение защищенности ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

2.3. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.4. Материальный носитель информации – материальный объект, используемый для закрепления и хранения на нем речевой, звуковой или изобразительной информации, в том числе в преобразованном виде.

2.5. Неавтоматизированная обработка ПДн (обработка ПДн без использования средств автоматизации) – обработка ПДн, при которой такие действия с ПДн, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого субъекта ПДн осуществляются при непосредственном участии человека. Обработка ПДн не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержатся в ИСПДн, либо были извлечены из нее.

2.6. Обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн. Действия (операции) с ПДн:

- сбор – действия (операции), направленные на получение ПДн;
- запись – действия (операции), направленные на фиксирование ПДн на материальных носителях и в ИСПДн;
- систематизация – действия (операции) по группировке ПДн;
- накопление – действия (операции) по сбору ПДн и формированию баз данных ПДн;
- хранение – действия (операции) с ПДн, направленные на создание условий для сохранности ПДн, включая их защиту от несанкционированного доступа до момента, когда ПДн должны быть уничтожены;
- извлечение – действия (операции), направленные на выборку ПДн из других сведений;

– уточнение (обновление, изменение) – действия (операции) с ПДн, совершаемые в целях их актуализации в случае изменения ПДн;

– использование – действия (операции) с ПДн, совершаемые в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц;

– распространение – действия, направленные на раскрытие ПДн неопределенному кругу лиц, в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом;

– предоставление – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

– доступ – действия, направленные на предоставление доступа к ПДн;

– обезличивание – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

– блокирование – действия, направленные на временное прекращение обработки ПДн (за исключением случаев, если обработка ПДн необходима для уточнения ПДн);

– удаление, уничтожение – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и/или в результате которых уничтожаются материальные носители ПДн.

2.7. Иные понятия, применяемые в настоящих Правилах, используются в значениях, определенных законодательством Российской Федерации в области обработки и защиты ПДн и нормативными правовыми актами города Москвы.

3. Цели обработки персональных данных и субъекты персональных данных

3.1. Обработка персональных данных осуществляется ГБУЗ «ДКЦ № 1 ДЗМ» в следующих целях:

3.1.1. Обеспечение соблюдения федеральных законов и иных нормативных актов Российской Федерации и города Москвы, регулирующих вопросы ведения бухгалтерского, налогового и воинского учета, кадровой работы при прохождении гражданами государственной гражданской службы города Москвы в Организации.

3.1.2. Обеспечение соблюдения федеральных законов и иных нормативных правовых актов Российской Федерации, регулирующих вопросы участия граждан в конкурсах на включение в кадровый резерв и замещение вакантных должностей государственной гражданской службы города Москвы в Организации.

3.1.3. Оформление доверенностейработникам.

3.1.4. Проведение закупок в соответствии с требованиями Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

3.1.5. Заключение и исполнение государственных контрактов с контрагентами.

3.1.6. Обеспечение соблюдения федеральных законов и иных нормативных, правовых актов, регламентирующих правоотношения в сфере рассмотрения обращений физических и юридических лиц, обеспечение доступа к информации о деятельности государственных органов.

3.1.7. Предоставление государственных или муниципальных услуг и осуществления государственных или муниципальных функций.

3.2. Для целей обработки персональных данных, указанных в пунктах 3.1.1-3.1.6 настоящих Правил, ГБУЗ «ДКЦ № 1 ДЗМ» является оператором ПДн, организующим и (или) осуществляющим обработку ПДн, формируемых при осуществлении полномочийГБУЗ «ДКЦ № 1 ДЗМ», а также определяющим цели и содержание обработки таких ПДн, действия (операции), совершаемые с ними.

3.3. Перечень обрабатываемых ПДн для целей, указанных в пунктах 3.1.1-3.1.6 настоящих Правил, закреплен в Перечне персональных данных, обрабатываемых в ГБУЗ «ДКЦ № 1 ДЗМ», утверждаемом ГБУЗ «ДКЦ № 1 ДЗМ» в установленном порядке. Пересмотр содержания Перечня персональных данных, обрабатываемых в ГБУЗ «ДКЦ № 1 ДЗМ» проводится по необходимости, но не реже одного раза в 3 года.

3.4. При организации обработки ПДн в целях, предусмотренных пунктами 3.1.1 – 3.1.6 настоящих Правил, ГБУЗ «ДКЦ № 1 ДЗМ» осуществляется обработка ПДн путем: сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), блокирования, удаления, уничтожения ПДн.

3.5. Для цели обработки ПДн, указанной в пункте 3.1.7 настоящих Правил, ГБУЗ «ДКЦ № 1 ДЗМ» является оператором ИСПДн, и обеспечивает эксплуатацию ИСПДн, выполняя обработку ПДн в части записи, хранения и передачи с использованием средств автоматизации, при этом перечень обрабатываемых ПДн, перечень других действий, совершаемых при их обработке, перечень лиц, осуществляющих обработку ПДн, правила обработки ПДн в ИСПДн определяются оператором ПДн, обрабатываемых в этих ИСПДн.

3.6. Перечень информационных систем, в которых осуществляется обработка ПДн, закреплен в Перечне информационных систем персональных данных ГБУЗ «ДКЦ № 1 ДЗМ», утверждаемом ГБУЗ «ДКЦ № 1 ДЗМ» в установленном порядке.

3.7. К субъектам ПДн, чьи данные обрабатываются в ГБУЗ «ДКЦ № 1 ДЗМ», относятся: *представители организаций – участников закупок, проводимых Организацией в соответствии с требованиями федерального закона от 05 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – участники закупок);*

– *представители контрагентов;*

– *физические лица, обратившиеся в Организацию с жалобой, предложением, заявлением или направившие запрос о предоставлении информации о деятельности Организации, ее подведомственных учреждений и предприятий;*

– *физические лица, предоставившие свои персональные в рамках исполнения Организацией своих полномочий.*

4. Основные правила обработки персональных данных

4.1. Обработка ПДн может осуществляться ГБУЗ «ДКЦ № 1 ДЗМ» в случаях, установленных законодательством Российской Федерации в сфере ПДн, в том числе в случаях, когда:

4.1.1. Обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн в случаях, установленных законодательством Российской Федерации.

4.1.2. Обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на ГБУЗ «ДКЦ № 1 ДЗМ» функций, полномочий и обязанностей.

4.1.3. Обработка ПДн необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти города Москвы и иных субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта ПДн в государственной информационной системе «Портал государственных и муниципальных услуг (функций) города Москвы».

4.1.4. Обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем.

4.1.5. Обработка ПДн необходима для осуществления прав и законных интересов ГБУЗ «ДКЦ № 1 ДЗМ» или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн.

4.1.6. Осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе.

4.1.7. Осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации и города Москвы.

4.2. В целях обеспечения прав и свобод человека и гражданина при обработке ПДн ГБУЗ «ДКЦ № 1 ДЗМ» обязана соблюдать следующие общие требования:

4.2.1. При определении объема и содержания обрабатываемых ПДн ГБУЗ «ДКЦ № 1 ДЗМ» должна руководствоваться законодательством Российской Федерации и нормативными правовыми актами города Москвы.

4.2.2. Все ПДн следует получать непосредственно у субъекта ПДн, за исключением случаев, когда право ГБУЗ «ДКЦ № 1 ДЗМ» на получение ПДн иным способом установлено законодательством Российской Федерации в сфере ПДн и правовыми актами, принимаемыми в соответствии с данным законодательством или по поручению оператора ПДн.

Если предоставление ПДн является обязательным в соответствии с федеральным законом, но субъект ПДн отказывается их предоставить, необходимо разъяснить субъекту ПДн юридические последствия такого отказа.

4.2.3. Если ПДн получены не от субъекта ПДн, то до начала обработки таких ПДн необходимо предоставить субъекту ПДн информацию, определенную ч.3 ст.18 Федерального закона № 152-ФЗ «О персональных данных», за исключением случаев, предусмотренных ч.4 ст.18 требований Федерального закона № 152-ФЗ «О персональных данных».

4.2.4. В случае передачи ПДн третьей стороне обязательным требованием является наличие согласия субъекта ПДн, за исключением случаев, установленных законодательством Российской Федерации и нормативными правовыми актами города Москвы.

4.2.5. ГБУЗ «ДКЦ № 1 ДЗМ» не имеет права получать и обрабатывать ПДн о его членстве в общественных объединениях, за исключением случаев, предусмотренных законодательством Российской Федерации, нормативными правовыми актами города Москвы.

4.2.6. ПДн не могут быть использованы в целях причинения имущественного и морального вреда субъекту ПДн, ограничения реализации его прав и свобод.

4.3. Доступ к ПДн:

4.3.1. Перечень должностей работников ГБУЗ «ДКЦ № 1 ДЗМ», осуществляющих обработку ПДн, закреплен в «Перечне должностей работников ГБУЗ «ДКЦ № 1 ДЗМ», замещение которых предусматривает осуществление обработки персональных данных», утверждаемом ГБУЗ «ДКЦ № 1 ДЗМ» в установленном порядке.

4.3.2. Доступ к ПДн, обрабатываемым в ГБУЗ «ДКЦ № 1 ДЗМ», разрешается только работникам, должности которых включены в «Перечень должностей работников ГБУЗ «ДКЦ № 1 ДЗМ», замещение которых предусматривает осуществление обработки персональных данных» и только в необходимом объеме.

4.3.3. До начала обработки ПДн все работники ГБУЗ «ДКЦ № 1 ДЗМ» ознакомлены с положениями внутренних нормативных документов по вопросам обработки и обеспечения безопасности ПДн в ГБУЗ «ДКЦ № 1 ДЗМ» и подписывают Обязательство о неразглашении и обеспечении безопасности персональных данных.

4.3.4. До сведения работников ГБУЗ «ДКЦ № 1 ДЗМ», осуществляющих обработку ПДн, доводятся положения законодательства в сфере ПДн.

4.3.5. Работники ГБУЗ «ДКЦ № 1 ДЗМ», осуществляющие обработку ПДн без использования средств автоматизации, проинформированы:

- о факте обработки ими ПДн, осуществляемой без использования средств автоматизации;
- о категориях обрабатываемых ПДн;
- об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами, в том числе, федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также внутренними документами ГБУЗ «ДКЦ № 1 ДЗМ»;

– об ответственности в случае нарушении норм, регулирующих обработку и защиту ПДн, установленных законодательством Российской Федерации.

5. Правила обмена персональными данными с третьими лицами

5.1. ГБУЗ «ДКЦ № 1 ДЗМ» в ходе своей деятельности может получать ПДн от третьих лиц и передавать ПДн третьим лицам в установленных целях.

5.2. Обмен ПДн может осуществляться в следующих случаях:

– в случае получения или отправки письменного запроса на предоставление ПДн;

– в случае, когда ГБУЗ «ДКЦ № 1 ДЗМ» поручает обработку ПДн третьему лицу;

– в случае, когда ГБУЗ «ДКЦ № 1 ДЗМ» поручается обработка ПДн;

– в случае, когда между ГБУЗ «ДКЦ № 1 ДЗМ» и третьим лицом заключен договор (соглашение) и ПДн необходимо предоставить для исполнения договора;

– в случае, когда обмен ПДн осуществляется в целях исполнения требований законодательства.

5.3. Запрос на предоставление ПДн:

5.3.1. В случае получения ГБУЗ «ДКЦ № 1 ДЗМ» запроса на предоставление ПДн проверяется законность такого запроса и принимается решение о возможности предоставления ПДн.

5.3.2. Порядок рассмотрения запросов субъектов ПДн и их представителей определен в Правилах рассмотрения запросов субъектов персональных данных и их представителей.

5.3.3. В случае, если ГБУЗ «ДКЦ № 1 ДЗМ» направляет запрос на предоставление ПДн, такой запрос должен содержать цель запроса, правовые основания запроса, перечень запрашиваемой информации.

Обмен ПДн по телефону, факсу, электронной почте осуществляется при соблюдении конфиденциальности и по защищенным каналам связи или в зашифрованном виде. Обмен ПДн по незащищенным каналам связи не допускается.

5.3.4. Ответы на письменные запросы третьих лиц в пределах их компетенции и предоставленных полномочий даются в письменной форме и в необходимом объеме.

5.4. Поручение ГБУЗ «ДКЦ № 1 ДЗМ» обработки ПДн третьему лицу:

5.4.1. ГБУЗ «ДКЦ № 1 ДЗМ» вправе поручить обработку ПДн третьему лицу. При этом должны быть определены цели обработки ПДн. Третье лицо не в праве осуществлять обработку ПДн в любых иных целях, кроме указанных в поручении на обработку.

Поручение органом исполнительной власти (ОИВ) обработки ПДн третьим лицам может осуществляться путем заключения государственного контракта либо путем принятия ОИВ соответствующего акта (поручение оператора). Существенным условием поручения оператора является обязанность обеспечения указанным лицом конфиденциальности и безопасности ПДн при их обработке.

5.4.2. Поручение на обработку ПДн должно содержать сведения, приведенные в ч.3 ст.6 Федерального закона № 152-ФЗ «О персональных данных».

5.4.3. ГБУЗ «ДКЦ № 1 ДЗМ» вправе поручить обработку ПДн только с согласия субъекта ПДн.

5.4.4. В случае если ГБУЗ «ДКЦ № 1 ДЗМ» поручает обработку ПДн третьему лицу, ответственность перед субъектом ПДн за действия указанного лица несет ГБУЗ «ДКЦ № 1 ДЗМ».

5.5. Поручение обработки ПДн ГБУЗ «ДКЦ № 1 ДЗМ»:

5.5.1. ГБУЗ «ДКЦ № 1 ДЗМ» может быть поручена обработка ПДн от другого лица, являющегося оператором ПДн, на основании заключаемого с этим лицом договора (государственного или муниципального контракта), либо путем принятия государственным или муниципальным органом соответствующего нормативного ГБУЗ «ДКЦ № 1 ДЗМ» является участником информационно-технологического взаимодействия.

5.5.2. ГБУЗ «ДКЦ № 1 ДЗМ» при осуществлении обработки ПДн по поручению оператора, обязана соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных».

5.5.3. ГБУЗ «ДКЦ № 1 ДЗМ» при осуществлении обработки ПДн по поручению оператора не обязана получать согласие субъекта ПДн на обработку его ПДн.

5.5.4. ГБУЗ «ДКЦ № 1 ДЗМ» при осуществлении обработки ПДн по поручению оператора несет ответственность перед оператором.

5.6. Обмен ПДн в рамках договорных отношений:

5.6.1. Договор между ГБУЗ «ДКЦ № 1 ДЗМ» и третьим лицом, в рамках исполнения которого будут предоставляться ПДн, должен содержать обязательство о соблюдении конфиденциальности ПДн.

5.7. Обмен ПДн на основании действующего законодательства

5.7.1. Получателями ПДн в соответствии с законодательством Российской Федерации являются Фонд социального страхования Российской Федерации, Пенсионный фонд Российской Федерации, Федеральная инспекция труда, налоговые органы, правоохранительные и судебные органы, органы статистики и иные органы надзора и контроля соблюдения законодательства о труде.

6. Хранение персональных данных

6.1. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

6.2. Сроки хранения ПДн в ГБУЗ «ДКЦ № 1 ДЗМ» определяются исходя из целей обработки ПДн и в соответствии с требованиями федеральных законов Российской Федерации.

6.3. Срок хранения ПДн в электронном виде не должен превышать срок хранения этих же данных на бумажных носителях.

6.4. При хранении ПДн на машинных носителях ГБУЗ «ДКЦ № 1 ДЗМ» обеспечивается регулярное резервное копирование информации с целью недопущения потери ПДн при выходе из строя машинных носителей ПДн.

7. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

7.1. В ГБУЗ «ДКЦ № 1 ДЗМ» ПДн уничтожаются в следующих случаях:

- достижения цели обработки ПДн (в том числе по истечении установленных сроков хранения);
- отзыва субъектом ПДн согласия на обработку своих ПДн, когда это согласие является обязательным условием обработки ПДн;
- невозможности устранения допущенных при обработке ПДн нарушений;
- получения соответствующего предписания от уполномоченного органа по защите прав субъектов ПДн.

7.2. Лица, осуществляющие обработку ПДн на бумажных и электронных носителях, осуществляют систематический контроль и выделение документов и сведений, содержащих ПДн, с истекшими сроками хранения, подлежащих уничтожению.

7.3. Уничтожение документов и сведений с истекшим сроком хранения осуществляется в установленном в ГБУЗ «ДКЦ № 1 ДЗМ» порядке.

7.4. Сроки уничтожения ПДн в случаях, приведенных в п.7.1 настоящих Правил, определяются ст.21 ФЗ-152 Федерального закона № 152-ФЗ «О персональных данных»:

7.5. Уничтожение ПДн на бумажных и электронных носителях производится путем, не позволяющим произвести считывание или восстановление ПДн.

7.6. Уничтожение ПДн осуществляется комиссией, назначаемой приказом (распоряжением) по ГБУЗ «ДКЦ № 1 ДЗМ».

7.7. По результатам уничтожения составляется Акт уничтожения персональных данных в ГБУЗ «ДКЦ № 1 ДЗМ».

8. Правила обработки персональных данных, осуществляемой без использования средств автоматизации

8.1. При неавтоматизированной обработке ПДн на материальных носителях должны выполнятся требования, установленные Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687.

8.2. При работе с материальными носителями ПДн должны выполняться следующие правила:

8.2.1. Хранение материальных носителей ПДн допускается только в тех помещениях и хранилищах (шкафах, сейфах), которые указаны в «Перечне мест хранения материальных носителей персональных данных в ГБУЗ «ДКЦ № 1 ДЗМ». В случае необходимости организации нового хранилища, соответствующие изменения вносятся в Перечень мест хранения материальных носителей персональных данных.

8.2.2. Материальные носители ПДн должны храниться в сейфах или запирающихся шкафах. Постоянное хранение материальных носителей ПДн в ящиках столов, открытых шкафах и других, не предназначенных для этого местах, не допускается.

8.2.3. Неконтролируемое пребывание посторонних лиц в помещениях, в которых хранятся материальные носители ПДн, не допускается. На время отсутствия работников на рабочем месте помещения должны запираться.

8.2.4. Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях[1].

8.2.5. За сохранность конкретного материального носителя ПДн отвечает работник, получивший этот материальный носитель в пользование.

8.2.6. В целях обеспечения сохранности и безопасности материальных носителей ПДн работникам ГБУЗ «ДКЦ № 1 ДЗМ» запрещается:

- разглашать содержимое материальных носителей ПДн;
- передавать материальные носители ПДн лицам, не имеющим права доступа к ним;
- несанкционированно вносить какие-либо изменения в содержимое материальных носителей ПДн;
- использовать материальные носители ПДн, подлежащие уничтожению;
- оставлять материальные носители ПДн на столах и в других легкодоступных местах при отсутствии работника на рабочем месте;
- несанкционированно копировать и/или тиражировать материальные носители ПДн;
- несанкционированно выносить материальные носители ПДн за пределы служебных помещений.

8.2.7. Вывод на печать документов, содержащих ПДн, допускается в связи с исполнением служебных обязанностей, в том числе в целях передачи печатных копий субъектам ПДн либо лицам, допущенным в соответствии с настоящими Правилами к работе с ПДн.

8.2.8. При печати ПДн на материальные носители ПДн запрещается оставлять материальные носители ПДн в принтере после печати.

9. Обеспечение защиты персональных данных

9.1. Защита ПДн обеспечивается совокупностью организационных, технических и правовых мероприятий, необходимых для обеспечения уровня защищенности ПДн, установленного законодательством Российской Федерации и внутренними документами ГБУЗ «ДКЦ № 1 ДЗМ», в том числе ограничением доступа к ПДн и в помещения, в которых осуществляется обработка ПДн.

9.2. Защите подлежит:

- документы, содержащие ПДн на бумажных носителях;

---

[1] Допускается хранение таких материальных носителей ПДн в одном шкафу на различных полках При этом материальные носители ПДн должны быть сгруппированы по целям обработки зафиксированных на них ПДн.

– ПДн, содержащиеся на электронных носителях и (или) в информационных системах.

9.3. Лица, осуществляющие обработку ПДн на бумажных и электронных носителях, обеспечивают их защиту от несанкционированного доступа и копирования в соответствии с требованиями законодательства Российской Федерации в сфере ПДн, внутренних документов ГБУЗ «ДКЦ № 1 ДЗМ» по вопросам обработки и защиты ПДн.

9.4. Обрабатываемые ПДн подлежат защите от актуальных угроз безопасности информации. Безопасность ПДн при их обработке обеспечивается путем принятия правовых, организационных и технических мер, направленных на защиту ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении ПДн.

9.5. Обеспечение безопасности ПДн достигается:

– определением угроз безопасности ПДн при их обработке в информационных системах персональных данных;

– применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы персональных данных;

– учетом машинных носителей ПДн;

– обнаружением фактов несанкционированного доступа к ПДн и принятием мер;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к ПДн, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в информационной системе персональных данных;

– контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности ПДн, обрабатываемых в информационных систем персональных данных.

10. Права субъектов персональных данных

Субъекты ПДн, данные которых обрабатываются в ГБУЗ «ДКЦ № 1 ДЗМ», имеют право:

– получать у ГБУЗ «ДКЦ № 1 ДЗМ» полную информацию, касающуюся обработки его ПДн;

– осуществлять свободный бесплатный доступ к своим ПДн, включая право получать копии любой записи, содержащей ПДн, за исключением случаев, предусмотренных законодательством Российской Федерации и города Москвы;

– требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– обжаловать действия или бездействие ГБУЗ «ДКЦ № 1 ДЗМ» в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) или в судебном порядке в случае, если субъект ПДн считает, что ГБУЗ «ДКЦ № 1 ДЗМ» осуществляет обработку его ПДн с нарушением требований Федерального закона № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы;

– на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке;

– осуществлять иные действия, предусмотренные законодательством Российской Федерации в сфере ПДн.

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

ПРАВИЛА
рассмотрения ГБУЗ «ДКЦ № 1 ДЗМ» запросов субъектов персональных данных или их представителей

1 Общие положения

1.1 Настоящие правила рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила) определяют порядок рассмотрения запросов субъектов персональных данных или их представителей **ГБУЗ «ДКЦ № 1 ДЗМ»** в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»).

1.2 Настоящими Правилами рассматриваются порядок реагирования на следующие запросы субъектов персональных данных:

– получение информации, касающейся обработки персональных данных субъекта персональных данных;

– уточнение персональных данных субъекта персональных данных, если они являются неполными, устаревшими, неточными, незаконно полученными либо не являются необходимыми для заявленной цели обработки;

– жалобы на неправомерную обработку ГБУЗ «ДКЦ № 1 ДЗМ» персональных данных субъекта персональных данных;

– отзыв согласия субъекта персональных данных на обработку персональных данных.

1.3 Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области защиты персональных данных (далее - ПДн).

1.4 Правила обязательны для исполнения всеми работниками **ГБУЗ «ДКЦ № 1 ДЗМ»**, организующими или непосредственно участвующими в процессе обработки запросов субъектов ПДн и их представителей.

2 Общий порядок рассмотрения запросов

2.1 Организация обработки обращений субъектов ПДн возлагается на *Ответственного за организацию обработки ПДн*.

2.2 Взаимодействие с работниками **ГБУЗ «ДКЦ № 1 ДЗМ»** осуществляется структурным подразделением, ответственным за кадровое делопроизводство.

2.3 Запрос субъекта ПДн (представителя субъекта ПДн) может быть направлен в **ГБУЗ «ДКЦ № 1 ДЗМ»**:

– в письменной форме;

– в форме электронного документа, подписанного электронной подписью в соответствии с законодательством Российской Федерации.

2.4 Все поступившие запросы субъектов ПДн (представителей субъекта ПДн) по вопросам обработки ПДн регистрируются в Журнале учета обращений субъектов персональных данных и представителей субъектов персональных данных **ГБУЗ «ДКЦ № 1 ДЗМ»** (Приложение 1 к настоящим Правилам).

2.5 Ответственным лицом за ведение Журнала учета обращений субъектов ПДн и представителей субъектов ПДн **ГБУЗ «ДКЦ № 1 ДЗМ»** является *Ответственный за организацию обработки ПДн*.

2.6 После регистрации запрос передается на исполнение для подготовки мотивированного ответа. Перечень лиц, привлекаемых для подготовки ответа, определяется в зависимости от предмета обращения.

2.7 В **ГБУЗ «ДКЦ № 1 ДЗМ»** организовано хранение следующих документов в течении трех лет:

– запросы субъекта ПДн или его представителя;

– копии документов, являющихся основанием для уточнения или отказа в уточнении обрабатываемых ПДн, для прекращения неправомерной обработки ПДн или отказа в прекращении обработки ПДн, для отказа в прекращении обработки ПДн;

– копии уведомления субъекта ПДн или его представителя об уточнении или отказе в уточнении обрабатываемых ПДн;

– копии уведомления субъекта ПДн или его представителя о прекращении неправомерной обработки ПДн или отказе в прекращении обработки ПДн;

– копии уведомления субъекта ПДн или его представителя о прекращении обработки ПДн или отказе в прекращении обработки ПДн;

– иные документы и копии иных документов, непосредственно связанные с выполнением ГБУЗ «ДКЦ № 1 ДЗМ» своих обязанностей по рассмотрению запросов субъекта ПДн или его представителя.

2.8 Лица, задействованные в подготовке ответа, должны соблюдать порядок и сроки обработки запросов, установленные законодательством Российской Федерации в зависимости от их типов (Приложение 2 к настоящим Правилам).

2.9 *Ответственный за организацию обработки ПДн* контролирует соблюдение указанных сроков в соответствии с законодательством Российской Федерации.

2.10 После подготовки и отправки ответа на запрос делается соответствующая отметка в Журнале учета обращений субъектов ПДн и представителей субъектов ПДн **ГБУЗ «ДКЦ № 1 ДЗМ»** с указанием даты отправки.

3 Запросы на предоставление информации, касающейся обработки персональных данных

3.1 В случае поступления от субъекта ПДн (представителя субъекта ПДн) запроса о предоставлении сведений, касающихся обработки ПДн, **ГБУЗ «ДКЦ № 1 ДЗМ»** подготавливает согласно запросу необходимый ответ. Перечень сведений, которые может запрашивать субъект ПДн (представитель субъекта ПДн) установлен ст.14 ФЗ «О персональных данных».

3.2 Запрос субъекта ПДн о предоставлении сведений, касающихся обработки его ПДн, должен содержать сведения, указанные в ч.3 ст.14 ФЗ «О персональных данных».

3.3 В случае требования предоставления иных, не предусмотренных законодательством сведений, **ГБУЗ «ДКЦ № 1 ДЗМ»** подготавливает мотивированный отказ в предоставлении сведений со ссылкой на законодательство Российской Федерации.

3.4 Выдача работникам **ГБУЗ «ДКЦ № 1 ДЗМ»** документов, связанных с их трудовой деятельностью (копий приказов о приеме на работу, переводах на другую работу, увольнении с работы; выписок из трудовой книжки, справок о месте работы, заработной плате, периоде работы в организации и др.) регулируется трудовым законодательством Российской Федерации и внутренними нормативными документами **ГБУЗ «ДКЦ № 1 ДЗМ».**

4 Отзыв согласия субъекта персональных данных на обработку персональных данных

4.1 При поступлении запроса (обращения), направленного на отзыв согласия на обработку ПДн, обращение (запрос) рассматривается на предмет возможности прекращения обработки ПДн этого субъекта в текущий момент.

Если запрос направлен на прекращение обработки ПДн в ИСПДн, в отношении которых **ГБУЗ «ДКЦ № 1 ДЗМ»** *является оператором, то такой запрос передается в орган исполнительный власти города Москвы, который является оператором ПДн, обрабатываемых в ИСПДн.*

4.2 В случае принятия решения о возможности прекращения обработки ПДн данные уничтожаются (либо обеспечивается их уничтожение) в соответствии с требованиями законодательства Российской Федерации в срок, не превышающий 30 (тридцати) дней с даты поступления указанного отзыва, если иное не предусмотрено договором, иным соглашением между ГБУЗ «ДКЦ № 1 ДЗМ» и субъектом ПДн либо если ГБУЗ «ДКЦ № 1 ДЗМ» не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством Российской Федерации.

В случае если возможно прекратить обработку только части ПДн, уничтожается часть обрабатываемых Организацией ПДн субъекта. Далее подготавливается ответ об уничтожении части обрабатываемых Организацией ПДн субъекта, и о том, что в соответствии с пп.2-11 ч.1 ст.6 ФЗ «О персональных данных» Организация вправе продолжить обработку оставшейся части ПДн субъекта без согласия субъекта ПДн до окончания сроков обработки ПДн.

4.3 В случае если прекратить обработку ПДн не представляется возможным по требованиям законодательства, формируется ответ субъекту ПДн (его представителю) о том, что ГБУЗ «ДКЦ № 1 ДЗМ» в соответствии с пп. 2-11 ч.1 ст.6 ФЗ «О персональных данных» праве продолжить обработку ПДн без согласия субъекта ПДн.

5 Запросы субъектов ПДн на уточнение их персональных данных

5.1 При поступлении запроса (обращения) об уточнении ПДн, которые являются неполными, устаревшими или неточными, должна быть инициирована процедура блокирования ПДн этого субъекта (если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц). Далее запрос анализируется на предмет возможности уточнения указанных в запросе ПДн.

5.2 В случае подтверждения факта неточности ПДн на основании сведений, представленных субъектом ПДн (его представителем) вносят необходимые изменения в ПДн. Далее инициируется процедура разблокирования ПДн и субъект ПДн (его представитель) информируется о произведенных изменениях.

В случае если факт неточности ПДн не подтвержден документально, инициируется процедура разблокирования ПДн, после чего формируют ответ субъект ПДн (его представитель) информируется об отсутствии возможности внесения изменений в ПДн.

5.3 При поступлении обращения (запроса) об уничтожении ПДн субъекта, которые были незаконно получены или не являлись необходимыми для заявленной цели обработки, инициируется процедура блокирования ПДн этого субъекта. Далее принимается решение по вопросу о правомерности обращения (запроса).

5.4 В случае принятия решения об отказе[1] субъекту ПДн разблокируются и субъект ПДн (его представитель) уведомляется о причинах отказа. В случае принятия решения о правомерности обращения (запроса) осуществляется уничтожение ПДн, указанных в обращении (запросе) и субъекту ПДн (его представителю) направляется ответ об удовлетворении его требований.

5.5 В случае необходимости информирование уполномоченного органа по защите прав субъектов ПДн осуществляется по почте в адрес указанного органа.

6 Запросы субъектов персональных данных с жалобами на неправомерную обработку их персональных данных

6.1 После поступления запроса (обращения) с жалобами на неправомерную обработку инициируется процедура блокирования (или обеспечивается блокирование ПДн) ПДн субъекта, направившего обращение (запрос) и проводится проверка по данному факту. В ходе проверки рассматривается правомерность обращения (запроса) и принимается решение по дальнейшим действиям по обращению (запросу) – устранить нарушение, уничтожить ПДн в случае невозможности устранения, отказать субъекту ПДн.

6.2 В случае принятия положительного решения нарушения устраняются и субъект ПДн (его представитель) оповещается об устранении нарушений.

6.3 В случае невозможности устранить нарушения ПДн, указанные в обращении (запросе) уничтожаются, и субъект ПДн (его представитель) оповещаются о данном факте.

6.4 В случае принятия решения об отказе субъекту инициируется процедура разблокирования ПДн и субъекту ПДн (его представителю) направляется ответ с обоснованием отказа.

6.5 В случае необходимости информирование уполномоченного органа по защите прав субъектов ПДн осуществляется по почте в адрес указанного органа.

---

[1] Отказ устранения нарушений должен быть мотивированным в соответствии с требованиями законодательства РФ.

Приложение 1
к Правилам рассмотрения запросов субъектов персональных данных или их представителей

УТВЕРЖДАЮ

_____ / _____

«____» _____ 20__ г.

ЖУРНАЛ
учета обращений субъектов персональных данных и представителей субъектов персональных данных
ГБУЗ «ДКЦ № 1 ДЗМ»

Начат: «___» _____ 20___ г. На ____ листах

Окончен: «___» _____ 20___ г.

_____ _____
(ФИО ответственного лица за ведение журнала) подпись

Москва 20__

№ п/п	Фамилия И.О. обратившегося лица	Документы, подтверждающие полномочия обратившегося лица[2]	Сведения о запросе		Действие по обращению	Сведения о принятом решении		Подпись исполнителя	Примечания
			Дата поступления запроса	Предмет		Дата отправки ответа	Основание		
1.[3]	*Петров П.П.*	*Паспорт РФ*	*01.03.2016*	*Уничтожение ПДн*	*Осуществлено уничтожение ПДн*	*28.03.2018*	*ч. 3 ст. 21 ФЗ «О персональных данных»*		

[2] Субъект персональных данных предоставляет документ, удостоверяющий личность. Представитель субъекта персональных данных предоставляет документ, удостоверяющий личность, и доверенность или иной документ, подтверждающий полномочия этого представителя.

[3] В строке приведен пример заполнения Журнала.

Приложение 2
к Правилам рассмотрения ГБУЗ «ДКЦ № 1 ДЗМ»
запросов субъектов персональных данных
или их представителей

Порядок и сроки обработки запросов и обращений субъектов персональных данных на получение информации, касающейся обработки персональных данных

В таблицах 1–6 рассматриваются возможные случаи, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», когда субъект ПДн (представитель субъекта ПДн) может обратиться или направить запрос [*Наименование Организации*]. В каждой таблице описан порядок действий при реагировании на запросы и обращения субъектов ПДн (представителей субъектов ПДн), а также сроки выполнения указанных действий.

Таблица 1 – Сроки выполнения запроса и обращения субъекта ПДн (представителя субъекта ПДн) на получение информации, касающейся обработки ПДн

№ п/п	Действие	Срок выполнения действия	Примечание
1	Предоставить субъекту ПДн или его представителю запрашиваемую информацию, касающуюся обработки его ПДн, и предоставить возможность ознакомления с этими ПДн (согласно ст.14, 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»	В течение 30 дней со дня получения запроса субъекта ПДн или его представителя	Запрашиваемая информация не может быть предоставлена субъекту ПДн или его представителю в случаях, предусмотренных в п.8 ст.14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
2	Если запрашиваемая информация не может быть предоставлена субъекту ПДн или его представителю в соответствии с п.8 ст.14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», дать в письменной форме мотивированный ответ	В срок, не превышающий 30 дней со дня со дня получения запроса или обращения субъекта ПДн или его представителя	Мотивированный ответ должен содержать ссылку на п.8 ст.14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или на иной федеральный закон, являющийся основанием для отказа

Таблица 2 – Возможные сроки направления субъектом ПДн (представителем субъекта ПДн) повторного запроса или обращения на получение информации, касающейся обработки ПДн

№ п/п	Действие	Срок выполнения действия	Примечание
1	Если запрашиваемая информация и/или обрабатываемые ПДн были предоставлены в полном объеме, субъект ПДн вправе обратиться повторно к [*Наименование Организации*] или направить ему повторный запрос в целях получения информации, касающейся обработки его ПДн, и ознакомления с такими ПДн	Не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса	Если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн
2	Если запрашиваемая информация и/или обрабатываемые ПДн не были предоставлены в полном объеме, субъект ПДн вправе обратиться повторно к [*Наименование Организации*] или направить ему повторный запрос в целях получения информации, касающейся обработки его ПДн, и ознакомления с такими ПДн	В любое время	Повторный запрос должен содержать обоснование направления такого запроса

Таблица 3 – Сроки выполнения запроса и обращения субъекта ПДн (представителя субъекта ПДн) на уточнение его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными

№ п/п	Действие	Срок выполнения действия	Примечание
1	Блокировать на период проверки ПДн, относящиеся к субъекту ПДн, или обеспечить	Сразу после получения запроса или обращения	Если блокирование ПДн не нарушает права и

№ п/п	Действие	Срок выполнения действия	Примечание
	их блокирование лицом, действующим по поручению [*Наименование Организации*]	от субъекта ПДн или его представителя	законные интересы субъекта ПДн или третьих лиц
2	Если подтвержден факт обработки неполных, устаревших, неточных ПДн, уточнить ПДн или обеспечить их уточнение лицом, действующим по поручению [*Наименование Организации*] на основании предоставленных сведений, подтверждающих, что ПДн субъекта являются неполными, неточными или неактуальными, и снять блокирование ПДн	В срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными	-
3	Уведомить субъекта ПДн или его представителя о внесенных изменениях, а также принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы	Сразу после внесения изменений в ПДн	-

Таблица 4 – Сроки выполнения запроса и обращения субъекта ПДн (представителя субъекта ПДн) на уточнение его ПДн, их блокирования или уничтожения в случае, если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки

№ п/п	Действие	Срок выполнения действия	Примечание
1	Уничтожить ПДн, которые являются незаконно полученными или не являются необходимыми для заявленной цели обработки	В срок, не превышающий 7 рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки	-
2	Уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах, а также уведомить третьих лиц, которым ПДн этого субъекта были переданы	Сразу после уничтожения ПДн	-

Таблица 5 – Сроки выполнения запроса и обращения субъекта ПДн (представителя субъекта ПДн) в случае выявления неправомерной обработки ПДн

№ п/п	Действие	Срок выполнения действия	Примечание
1	Блокировать на период проверки неправомерно обрабатываемые ПДн, относящиеся к субъекту ПДн, или обеспечить их блокирование лицом, действующим по поручению [*Наименование Организации*]	Сразу после получения запроса или обращения от субъекта ПДн или его представителя	-
2	Если подтвержден факт неправомерной обработки ПДн, прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению [*Наименование Организации*]	В срок, не превышающий 3 рабочих дня со дня выявления неправомерной обработки ПДн	-
3	Если обеспечение правомерности обработки ПДн невозможно, уничтожить неправомерно обрабатываемые ПДн или обеспечить их уничтожение лицом, действующим по поручению [*Наименование Организации*]	В срок, не превышающий 10 рабочих дней со дня выявления неправомерной обработки ПДн	-
4	Если отсутствует возможность уничтожения ПДн в течение срока, указанного в п.3 данной таблицы, блокировать ПДн или обеспечить их блокирование лицом, действующим по поручению [*Наименование Организации*] и обеспечить уничтожение ПДн	В срок не более чем 6 месяцев	Если иной срок не установлен федеральными законами
5	Уведомить субъекта ПДн или его представителя об устранении допущенных нарушений или об	После устранения допущенных нарушений/	-

№ п/п	Действие	Срок выполнения действия	Примечание
	уничтожении ПДн	после уничтожения ПДн	

Таблица 6 – Сроки выполнения запроса и обращения субъекта ПДн (представителя субъекта ПДн) в случае отзыва согласия на обработку ПДн

№ п/п	Действие	Срок выполнения действия	Примечание
1	Прекратить обработку ПДн или обеспечить прекращение такой обработки лицом, действующим по поручению [*Наименование Организации*]	Сразу после поступления отзыва согласия на обработку ПДн	-
2	Если сохранение ПДн более не требуется для целей обработки ПДн или если [*Наименование Организации*] не вправе осуществлять обработку ПДн без согласия субъекта ПДн, уничтожить ПДн или обеспечить их уничтожение лицом, действующим по поручению [*Наименование Организации*]	В срок, не превышающий 30 дней со дня поступления указанного отзыва	Если иные сроки не предусмотрены договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн
3	Если отсутствует возможность уничтожения ПДн в течение срока, указанного в п.2 данной таблицы, блокировать ПДн или обеспечить их блокирование лицом, действующим по поручению [*Наименование Организации*] и обеспечить уничтожение ПДн	В срок не более чем 6 месяцев	Если иной срок не установлен федеральными законами

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1 Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) устанавливают основания, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных требованиям, установленным Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными, правовыми актами Российской Федерации, города Москвы и ГБУЗ «ДКЦ № 1 ДЗМ».

1.2. Настоящие Правила разработаны в соответствии с законодательством Российской Федерации и города Москвы в области обработки и защиты персональных данных и иными правовыми актами, принимаемыми в соответствии с данным законодательством (далее – законодательство в сфере персональных данных).

1.3. Целями осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) является:

– оценка выполнения в **ГБУЗ «ДКЦ № 1 ДЗМ»** требований по обработке и защите персональных данных, установленных законодательством Российской Федерации, Правительства Москвы, а также правовыми актами **ГБУЗ «ДКЦ № 1 ДЗМ»**;

– выявление и предотвращение в **ГБУЗ «ДКЦ № 1 ДЗМ»** нарушений законодательства Российской Федерации и города Москвы в сфере персональных данных.

1.4. Внутренний контроль проводится комиссией, назначаемой в порядке, установленном в ГБУЗ «ДКЦ № 1 ДЗМ» (далее – Комиссия).

1.5. В состав Комиссии могут входить работники ГБУЗ «ДКЦ № 1 ДЗМ» и внешние эксперты. В проведении внутреннего контроля не могут участвовать работники ГБУЗ «ДКЦ № 1 ДЗМ», прямо или косвенно заинтересованные в его результатах.

1.6. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения внутреннего контроля, обеспечивают конфиденциальность персональных данных субъектов персональных данных.

1.7. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

2 Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. Внутренний контроль осуществляется ГБУЗ «ДКЦ № 1 ДЗМ» путем проведения проверок соблюдения требований законодательства в сфере персональных данных и внутренних документов ГБУЗ «ДКЦ № 1 ДЗМ» по обработке и защите персональных данных (далее по тексту – проверки).

2.2. Проверки проводятся непосредственно на месте обработки персональных данных путем:

– опроса либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных;

– проверки документов, относящихся к деятельности структурного подразделения в части обработки и (или) защиты персональных данных;

– проведения, при необходимости, инструментальных проверок защищенности информационных систем персональных данных.

2.3. Проверки в ГБУЗ «ДКЦ № 1 ДЗМ» разделяются на:

– плановые;

– внеплановые.

2.4. Плановые проверки проводятся не реже одного раза в год в соответствии с Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – План внутреннего контроля).

Форма плана внутреннего контроля определяется Организацией самостоятельно. План разрабатывается и утверждается ежегодно.

Примерный перечень возможных проверок в ходе внутреннего контроля:

– *проверка соответствия указанных в «Перечне персональных данных» ПДн фактически обрабатываемым в Организации;*

– *проверка соответствия установленных прав доступа к ПДн полномочиям в рамках трудовых обязанностей работников;*

– *проверка актуальности Перечня должностей работников, замещение которых предусматривает осуществление обработки ПДн;*

– *проверка актуальности Перечня мест хранения материальных носителей персональных данных;*

– *проверка подтверждения факта ознакомления работников с локальными актами Организации в области обработки и обеспечения безопасности ПДн;*

– *проверка наличия в поручениях оператора сведений, установленных ч.3 ст. 6 Федерального закона «О персональных данных»;*

– *проверка наличия законных целей и оснований обработки всех ПДн по всем категориям субъектов ПДн;*

– *проверка соответствия целей обработки содержанию и объему обрабатываемых ПДн;*

– *выборочные проверки уровня знания работниками организационно-распорядительных документов в области обработки и обеспечения безопасности ПДн;*

– *проверка соблюдения сроков хранения и порядка уничтожения носителей ПДн;*

– *проверка соблюдения процедур и сроков подготовки ответов на обращения субъектов ПДн в соответствии со ст.20 и 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;*

– *проверка наличия и (или) необходимости актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных о начале обработки ПДн;*

– *проверка соблюдения условий использования средств защиты информации, используемых для обеспечения защиты ПДн, входящих в зону ответственности Организации, предусмотренных эксплуатационной и технической документацией на них;*

– *проверка функционирования технических средств защиты информации, используемых при обеспечении защиты персональных данных, входящих в зону ответственности Организации;*

– *проверка выполнения мер по обеспечению безопасности ПДн при их обработке, определенных в соответствии с установленным уровнем защищенности ПДн при их обработке в ИСПДн, включая, но не ограничиваясь:*

- *проверка регулярности обновления средств антивирусной защиты (актуальности вирусных баз);*
- *проверка проведения резервного копирования программных средств, архивов, журналов, информационных активов, используемых и создаваемых в процессе эксплуатации ИСПДн;*
- *проверка установки обновлений безопасности программного обеспечения, в т.ч. программного обеспечения средств защиты информации;*
- *проверка регистрации событий информационной безопасности;*
- *проверка реализации процесса управления конфигурациями ИСПДн и системы защиты ПДн;*
- *проверка реализации процесса управления доступом к ресурсам ИСПДн;*

– *проверка правильности эксплуатации средств криптографической защиты информации при их использовании в Организации;*

– *проверка выполнения организационных и технических мероприятий по обеспечению пропускного режима на территорию Организации.*

Перечень и содержание проверок может корректироваться исходя из специфики деятельности Организации.

2.5. План внутреннего контроля разрабатывается *Ответственным за организацию обработки персональных данных*, либо по его поручению. Разработанный План внутреннего контроля утверждается в порядке, установленном в ГБУЗ «ДКЦ № 1 ДЗМ».

2.6. Количество плановых проверок зависит от:

– результатов проведения предыдущих проверок;

– критичности объекта (структурного подразделения, осуществляющего обработку и (или) защиту персональных данных, или процесса обработки персональных данных), по которому планируется проведение проверки;

– предложений руководства и специалистов структурных подразделений **ГБУЗ «ДКЦ № 1 ДЗМ».**

2.7. Внеплановые внутренние проверки могут проводиться в следующих случаях:

– по результатам расследования выявленных нарушений требований законодательства в сфере персональных данных;

– по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов персональных данных;

– при существенных изменениях процессов или процедур обработки и защиты персональных данных;

– при выявлении большого числа нарушений требований законодательства в сфере персональных данных или повторяемости одних и тех же нарушений от проверки к проверке;

– по указанию руководства **ГБУЗ «ДКЦ № 1 ДЗМ».**

2.8. Руководители проверяемых структурных подразделений к началу проведения проверок должны обеспечить:

– доступность необходимых для проведения проверок работников;

– доступность необходимых для проведения проверок материалов;

– доступ к информационным ресурсам, владельцами которых они являются;

– доступ в помещения, имеющие отношения к области проведения проверок.

2.9. Результат проведения внутреннего контроля фиксируются в Отчете по результатам проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее по тексту – Отчет).

2.10. В Отчете должны быть указаны как минимум:

– основание проверки;

– вид проверки (плановая/внеплановая);

– цель проведения проверки;

– выявленные нарушения.

2.11. Отчет подписывают члены Комиссии, председатель Комиссии.

2.12. По результатам проведения внутреннего контроля Комиссией проводится анализ выявленных нарушений и разрабатывается план действий по устранению выявленных нарушений.

2.13. Результаты проведения внутреннего контроля и план действий по устранению выявленных нарушений доводятся до сведения руководства ГБУЗ «ДКЦ № 1 ДЗМ» для принятия решений о необходимости проведения работ по устранению выявленных нарушений.

2.14. Решения о необходимости проведения работ по устранению выявленных нарушений подлежат реализации в порядке, установленном в ГБУЗ «ДКЦ № 1 ДЗМ». В целях контроля устранения выявленных нарушений Комиссия может проводить повторные проверки.

3 Права Комиссии

3.1. Комиссия для реализации своих полномочий имеет право:

- привлекать к проведению проверок работников **ГБУЗ «ДКЦ № 1 ДЗМ»**;
- запрашивать у работников **ГБУЗ «ДКЦ № 1 ДЗМ»** необходимую информацию;
- принимать меры по устранению выявленных нарушений;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в сфере персональных данных.

3.2. К проведению проверок могут привлекаться третьи лица на договорной основе в соответствии с действующим законодательством.

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

ПРАВИЛА
работы с обезличенными данными в ГБУЗ «ДКЦ № 1 ДЗМ»

1 Общие положения

1.1 Настоящие Правила работы с обезличенными данными в ГБУЗ «ДКЦ № 1 ДЗМ» (далее – Правила), определяют порядок обезличивания персональных данных, обрабатываемых в информационных системах персональных данных, в соответствии с требованиями и методами, установленными уполномоченным органом по защите прав субъектов персональных данных.

1.2 Настоящие Правила разработаны в соответствии с законодательством Российской Федерации в области обработки и защиты персональных данных.

1.3 В настоящих Правилах используются следующие термины и определения:

– обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

– деобезличивание данных – действия, в результате которых обезличенные данные принимают вид, позволяющий определить их принадлежность конкретному субъекту персональных данных;

– обезличенные данные – данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации;

– обработка обезличенных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации, с обезличенными данными, без применения их предварительного деобезличивания.

2 Условия обезличивания

2.1 Обезличивание персональных данных может быть проведено с целью статистических или иных исследований, минимизацию рисков причинения вреда конкретным гражданам в случае утечки их персональных данных из информационных систем персональных данных, по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

3 Порядок обезличивания персональных данных

3.1 Обезличивание персональных данных в ГБУЗ «ДКЦ № 1 ДЗМ» осуществляется в случаях:

– передачи персональных данных третьему лицу, когда получателю персональных данных не требуется идентифицировать субъекта и для целей обработки достаточно обезличенных данных;

– интеграции информационной системы персональных данных **ГБУЗ «ДКЦ № 1 ДЗМ»** с другой информационной системой, когда в другой системе не требуется идентифицировать субъекта персональных данных и для целей интеграции достаточно передавать обезличенные данные;

– прекращения обработки персональных данных по достижении целей обработки персональных данных (при необходимости);

– обработки персональных данных в статистических или иных исследовательских целях.

3.2 В ГБУЗ «ДКЦ № 1 ДЗМ» могут применяться следующие методы обезличивания:

– метод введения идентификаторов – замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным;

– метод изменения состава или семантики – изменение состава или семантики персональных данных путем замены результатами статистической обработки, преобразования, обобщения или удаления части сведений;

– метод декомпозиции – разделение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;

– метод перемешивания – перестановка отдельных значений или групп значений атрибутов персональных данных в массиве персональных данных.

3.3 Процедура обезличивания персональных данных включает:

– выявление необходимости обезличивания персональных данных;

– назначение ответственного (ответственных) за проведение обезличивания персональных данных;

– определение метода обезличивания персональных данных;

– определение условий хранения и, при необходимости, передачи обезличенных данных.

3.4 Процедуру обезличивания персональных данных для каждого случая обезличивания устанавливают ответственные за проведения обезличивания персональных данных.

3.5 При выборе методов и процедур обезличивания персональных данных ГБУЗ «ДКЦ № 1 ДЗМ» необходимо руководствоваться целями и задачами обработки персональных данных.

3.6 Обезличивание персональных данных, обработка которых осуществляется с разными целями, может осуществляться разными методами.

3.7 При выборе метода и процедуры обезличивания необходимо учитывать:

– объем персональных данных, подлежащих обезличиванию (некоторые методы неэффективны на малых объемах);

– форму представления данных (отдельные записи, файлы, таблицы баз данных и т.д.);

– область обработки обезличенных данных (необходим ли другим операторам доступ к обезличиваемым данным);

– применяемые в информационной системе **ГБУЗ «ДКЦ № 1 ДЗМ»**меры по обеспечению безопасности данных.

4 Организация обработки обезличенных данных

4.1 При использовании ГБУЗ «ДКЦ № 1 ДЗМ» процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

4.2 В процессе обработки обезличенных данных ГБУЗ «ДКЦ № 1 ДЗМ», при необходимости, может проводиться деобезличивание. После обработки персональные данные, полученные в результате такого деобезличивания, должны быть уничтожены.

4.3 Должна быть обеспечена безопасность дополнительной (служебной) информации, содержащей параметры методов и процедур обезличивания/деобезличивания.

4.4 При реализации процедур обезличивания/деобезличивания, а также при последующей обработке обезличенных данных не должны нарушаться права субъекта персональных данных.

4.5 При хранении обезличенных данных необходимо:

– организовать раздельное хранение обезличенных данных и дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания;

– обеспечивать конфиденциальность дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания.

4.6 Передача по каналам передачи данных обезличенных данных совместно с информацией о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания ГБУЗ «ДКЦ № 1 ДЗМ» не допускается.

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в ГБУЗ «ДКЦ № 1 ДЗМ »

В «Перечне персональных данных, обрабатываемых в ГБУЗ «ДКЦ № 1 ДЗМ»*» приведены примеры заполнения граф формы. В Перечне указываются только те персональные данные (в привязке к процессам обработки ПДн, субъектам персональных данных, целям обработки), в отношении которых Организация является оператором ПДн и/или поставщиком информации (ответственной за информационное наполнение информационных систем).*

№ п/п	Категория субъектов персональных данных	Состав персональных данных	Правовые основания обработки	Сроки обработки (в т.ч. хранения)
1.	*Наименование процесса: Кадровый учет государственных гражданских служащих.* *Цели обработки персональных данных: обеспечение соблюдения федеральных законов и иных нормативных правовых актов Российской Федерации, регулирующих вопросы ведения кадровой работы при прохождении гражданами государственной гражданской службы города Москвы в ГБУЗ «ДКЦ № 1 ДЗМ.* *Способ обработки (неавтоматизированный/автоматизированный/смешанный): смешанный*			
1.1	*Государственные гражданские служащие*	– *фамилия, имя, отчество;* – *фотография;* – *гражданство;* – *дата и место рождения;* – *пол;* – *реквизиты документа, удостоверяющего личность;* – *адрес регистрации;* – *адрес проживания;* – *состояние в браке;* – *профессия;* – *сведения о трудовой деятельности;* – *стаж;* – *категория запаса;* – *сведения о воинском учете;* – *сведения об образовании;* – *номер страхового свидетельства государственного пенсионного страхования (СНИЛС);* – *идентификационный номер налогоплательщика (ИНН);* – *структурное подразделение;* – *должность;* – *оклад;* – *надбавка;* – *номер рабочего телефона;* – *серия и номер документа о повышении квалификации, переподготовке;* – *награды и номера документов, подтверждающих их получение;* – *социальные льготы;*	– *Трудовой кодекс Российской Федерации от 20 декабря 2001 г. № 197-ФЗ;* – *Федеральный закон от 27 июля 2004 г. №79-ФЗ «О государственной гражданской службе Российской Федерации»;* – *Закон города Москвы от 26 января 2005 г. №3 «О государственной гражданской службе города Москвы»;* – *Указ Президента Российской Федерации от 30 мая 2005 г. №609 «Об утверждении положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»*	*Срок обработки – на время прохождения гражданской службы и в течение 10 лет со дня увольнения с гражданской службы.* *Срок архивного хранения документов по личному составу, созданных после 2003 г. – 50 лет (Статья 22.1 Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»)* *Срок архивного хранения документов по личному составу, созданных до 2003 г. – 75 лет (Статья 22.1 Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»)*

12

№ п/п	Категория субъектов персональных данных	Состав персональных данных	Правовые основания обработки	Сроки обработки (в т.ч. хранения)
		– *статус работника (резидент/нерезидент);* – *сведения, содержащиеся в автобиография;* – *информация об участии в социальных сетях*		
1.2	*Ближайшие родственники государственных гражданских служащих*	– *фамилия, имя, отчество;* – *место жительства ближайших родственников;* – *дата и год рождения;* – *степень родства*	– *Трудовой кодекс Российской Федерации от 20 декабря 2001 г. № 197-ФЗ;* – *Федеральный закон «О государственной гражданской службе Российской Федерации» от 27 июля 2004 г. № 79-ФЗ;* – *Закон города Москвы от 26 января 2005 г. №3 «О государственной гражданской службе города Москвы»;* – *Указ Президента Российской Федерации от 30 мая 2005 г. №609 «Об утверждении положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»*	*Срок обработки – на время прохождения гражданской службы и в течение 10 лет со дня увольнения с гражданской службы.*
1.3	*Уволенные государственные гражданские служащие*	– *фамилия, имя, отчество;* – *фотография;* – *гражданство;* – *дата и место рождения;* – *пол;* – *реквизиты документа, удостоверяющего личность;* – *адрес регистрации;* – *адрес проживания;* – *состояние в браке;* – *профессия;* – *сведения о трудовой деятельности;* – *стаж;* – *категория запаса;* – *сведения о воинском учете;* – *сведения об образовании;* – *номер страхового свидетельства государственного пенсионного*	– *Трудовой кодекс Российской Федерации от 20 декабря 2001 г. № 197-ФЗ;* – *Федеральный закон «О государственной гражданской службе Российской Федерации» от 27 июля 2004 г. № 79-ФЗ;* – *Закон города Москвы «О государственной гражданской службе города Москвы» от 26 января 2005 г. №3;* – *Указ Президента Российской Федерации «Об утверждении положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» от 30 мая 2005 г. №609;* – *Постановление Правительства РФ от 8 сентября 2010 г. №700 «О порядке сообщения работодателем при заключении трудового договора с гражданином, замещавшим должности государственной или*	*Срок обработки – в течение 10 лет со дня увольнения с гражданской службы.* *Срок архивного хранения документов по личному составу, созданных после 2003 г. – 50 лет (Статья 22.1 Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»).* *Срок архивного хранения документов по личному составу, созданных до 2003 г. – 75 лет (Статья 22.1 Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»).*

№ п/п	Категория субъектов персональных данных	Состав персональных данных	Правовые основания обработки	Сроки обработки (в т.ч. хранения)
		страхования (СНИЛС) – *идентификационный номер налогоплательщика (ИНН);* – *структурное подразделение;* – *должность;* – *оклад;* – *надбавка;* – *номер рабочего телефона;* – *серия и номер документа о повышении квалификации, переподготовке;* – *награды и номера документов, подтверждающих их получение;* – *социальные льготы;* – *наличие инвалидности;* – *статус работника (резидент/нерезидент);* – *сведения, содержащиеся в автобиографии;* – *информация об участии в социальных сетях.*	*муниципальной службы, перечень которых устанавливается нормативными правовыми актами Российской Федерации, в течение 2 лет после его увольнения с государственной или муниципальной службы о заключении такого договора представителю нанимателя (работодателю) государственного или муниципального служащего по последнему месту его службы»*	
2.	*Наименование процесса: Бухгалтерская отчетность, расчет заработной платы, расчет налогов и социальных выплат.* *Цели обработки персональных данных: обеспечение соблюдения федеральных законов и иных нормативных правовых актов Российской Федерации, регулирующих вопросы ведения бухгалтерского, налогового учета, в т.ч. сдача отчетности в контролирующие органы, осуществление обязательных выплат и расчет заработной платы.* *Способ обработки (неавтоматизированный/автоматизированный/смешанный): смешанный*			
2.1	*Государственные гражданские служащие*	– *фамилия, имя, отчество;* – *дата рождения;* – *место рождения;* – *реквизиты документа, удостоверяющего личность;* – *адрес регистрации;* – *ИНН;* – *СНИЛС;* – *стаж;* – *сведения об образовании;* – *сведения о трудовой деятельности;* – *сведения о воинской обязанности;* – *свидетельство о браке;* – *свидетельства о рождении детей;* – *сведения о доходах.*	– *Трудовой кодекс Российской Федерации от 20 декабря 2001 г. № 197-ФЗ;* – *Налоговый кодекс Российской Федерации часть первая от 31 июля 1998 г. №146-ФЗ и часть вторая от 5 августа 2000 г. № 117-ФЗ;* – *Федеральный закон от 06 декабря 2011 г. № 402-ФЗ «О бухгалтерском учете»;* – *Федеральный закон от 01 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»*	*Сроки хранения бухгалтерской отчетности определяются в зависимости от формы учета и отчетности в соответствии со ст. 351- 463 приказа Минкультуры России от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения».*

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

ПЕРЕЧЕНЬ
должностей работников ГБУЗ «ДКЦ № 1 ДЗМ, замещение которых предусматривает осуществление обработки персональных данных

№ п/п	Наименование процесса	Должность
1.	*Кадровый учет работников Организации*	*Главный врач* *Заместитель главного врача* *Начальник Отдела кадров*
2.	*Бухгалтерская отчетность, расчет заработной платы, расчет налогов и социальных выплат*	*Главный врач* *Заместитель главного врача* *Главный бухгалтер* *Начальник планового отдела*

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

ПЕРЕЧЕНЬ
мест хранения материальных носителей персональных данных, обрабатываемых без использования средств автоматизации

№ п/п	Наименование процесса обработки персональных данных	Места хранения материальных носителей персональных данных (адрес)	Обрабатываемые категории персональных данных	Перечень лиц (должностей), которые осуществляют неавтоматизированную обработку персональных данных, либо имеют к ним доступ
1.	*Кадровый учет работников организации*	*г. Москва, ул. Миклухо-Маклая, д. 29, корп. 2.*	*Персональные данные, которые не могут быть отнесены к специальной[1] категории персональных данных, к биометрическим[2] персональным данным и к общедоступным[3] персональным данным (далее – иные категории персональных данных)*	*Главный врач* *Заместитель главного врача* *Начальник Отдела кадров*
2.	*Бухгалтерская отчетность, расчет заработной платы, расчет налогов и социальных выплат*	*г. Москва, ул. Миклухо-Маклая, д. 29, корп. 2.*	*Иные категории персональных данных*	*Главный врач* *Заместитель главного врача* *Начальник Отдела кадров* *Главный бухгалтер*

[1] Специальные категории персональных данных - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.
[2] Биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором персональных данных для установления личности субъекта персональных данных.
[3] Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

ОБЯЗАТЕЛЬСТВО
о неразглашении и обеспечении безопасности
персональных данных

Я, _____
(фамилия, имя, отчество)
_____
(должность)

обязуюсь:

1. Не разглашать, не распространять персональные данные субъектов персональных данных (далее – персональные данные), выполнять требования по обеспечению безопасности персональных данных, доступ к которым будет мне предоставлен или которые станут мне известны при выполнении должностных обязанностей.

2. Обеспечить конфиденциальность и безопасность персональных данных при их обработке как с использованием средств автоматизации, так и без использования таких средств (неавтоматизированная обработка).

3. Выполнять требования законодательства Российской Федерации, города Москвы, правовых актов и внутренних документов ГБУЗ «ДКЦ № 1 ДЗМ», иных документов, инструкций и положений, обязательных к исполнению и призванных обеспечить безопасность персональных данных.

4. Незамедлительно доводить до сведения непосредственного руководителя сведения:

1) о факте утраты (утери, хищения, недостачи) материальных носителей персональных данных, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, металлических шкафов, в которых хранятся персональные данные, личных печатей и о других фактах, которые могут привести к разглашению персональных данных;

2) о факте разглашения или неправомерной обработки персональных данных;

3) о ставших известными фактах или возможностях несанкционированного доступа к информационным системам, ресурсам, обрабатывающим персональные данные, о причинах и условиях возможной утечки персональных данных.

5. В случае моего увольнения:

5.1. Передать по акту непосредственному руководителю все носители, содержащие персональные данные (рукописи, черновики, распечатки на принтерах, флеш-накопители и иные электронные носители и др.), которые находились в моем распоряжении в связи с выполнением мною должностных обязанностей.

5.2. Не разглашать, не распространять, не использовать, не предпринимать возможности нарушений требований по обеспечению безопасности в течении трех лет после прекращения служебного (трудового) контракта, освобождения от замещаемой должности и увольнения к персональным данным, доступ к которым был мне предоставлен или которые были мне известны при выполнении должностных обязанностей.

6. Мне известно, что нарушение данных обязательств может повлечь уголовную, административную, гражданско-правовую или иную форму ответственности в соответствии с действующим законодательством Российской Федерации.

_____
(подпись)
«____»_____20__ г.

Я проинформирован(а) о факте обработки мной персональных данных в процессе выполнения моих должностных обязанностей, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки (как с использованием средств автоматизации, так и без использования таких средств), установленных законодательством Российской Федерации, города Москвы, иными подзаконными правовыми актами, правовыми актами (*применимо для органа исполнительной власти*), документами [*Наименование Организации*].

_____
(подпись)
«____»_____20__ г.

Я ознакомлен (а) с требованиями законодательства Российской Федерации, города Москвы и правовых актов, документов [*Наименование Организации*], регламентирующими порядок обработки и обеспечение безопасности персональных данных и обязуюсь на регулярной основе следить за изменениями указанных требований путем ознакомления с информацией, размещаемой работодателем на локальных ресурсах доступных служащим, работникам, допущенным к обработке персональных данных.

_____
(подпись)
«____»_____20__ г.

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

ОБЯЗАТЕЛЬСТВО
государственного гражданского служащего, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я, _____
(фамилия, имя, отчество)

_____,
(должность)

проходя государственную гражданскую службу в ГБУЗ «ДКЦ № 1 ДЗМ» осуществлял(а) непосредственную обработку персональных данных субъектов персональных данных (далее – персональные данные). При прекращении служебного контракта, освобождении от замещаемой должности государственной гражданской службы и увольнении с государственной гражданской службы в ГБУЗ «ДКЦ № 1 ДЗМ» я прекращаю обработку персональных данных и обязуюсь:

1. Передать по акту непосредственному руководителю все носители, содержащие персональные данные (рукописи, черновики, распечатки на принтерах, флеш-накопители и иные электронные носители и др.), которые находились в моем распоряжении в связи с выполнением мною должностных обязанностей.
2. В течении трех лет с даты прекращения служебного контракта, освобождения от замещаемой должности государственной гражданской службы и увольнения с государственной гражданской службы не разглашать, не распространять, не использовать, не допускать возможности нарушений требований по обеспечению безопасности персональных данных, доступ к которым был мне предоставлен или которые были мне известны при выполнении должностных обязанностей.

Мне известно, что нарушение данных обязательств может повлечь уголовную, административную, гражданско-правовую или иную форму ответственности в соответствии с действующим законодательством Российской Федерации.

_____ _____
(подпись) (Фамилия, инициалы)

«____»_____20__года

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

Форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

1. Разъяснение субъекту персональных данных при приеме на работу.

Мне, _____ разъяснены юридические последствия отказа предоставить свои персональные данные ГБУЗ «ДКЦ № 1 ДЗМ».

В соответствии со ст.65 Трудового Кодекса Российской Федерации, пп. «а» п.30 Положения о воинском учете, утвержденного Постановлением Правительства Российской Федерации от 27 ноября 2006 г. № 719, определен перечень документов, содержащих персональные данные, которые субъект персональных данных обязан предоставить ГБУЗ «ДКЦ № 1 ДЗМ» в связи с заключением трудового договора.

Без предоставления персональных данных, обязательных для заключения трудового договора, трудовой договор с субъектом персональных данных не может быть заключен.

_____/_____ «___»_____20__г.

(подпись) (ФИО)

2. Разъяснение субъекту персональных данных в иных случаях

Уважаемый_____

_____

(фамилия, имя, отчество субъекта персональных данных)

_____

(фамилия, имя, отчество представителя субъекта персональных данных, реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

_____

_____

(номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе)

_____

уведомляем Вас, что обязанность предоставления Вами персональных данных установлена:

_____

_____

_____

(основания предоставления персональных данных, установленные законодательством Российской Федерации)

В случае отказа Вами предоставить свои персональные данные ГБУЗ «ДКЦ № 1 ДЗМ»:

_____

_____

_____

_____

(юридические последствия отказа предоставления персональных данных)

_____ _____ _____

(должность) (подпись) (фамилия, имя, отчество)

_____

«____» _____ 20___ года

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

Ответственность за нарушение порядка обработки и обеспечения безопасности персональных данных

1. Дисциплинарная ответственность

Согласно статье 24 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», лица, виновные в нарушении требований Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

Согласно статье 90 Трудового кодекса Российской Федерации от 20 декабря 2001г. № 197-ФЗ, лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Статьей 81 Трудового кодекса Российской Федерации от 20 декабря 2001 г. № 197-ФЗ предусмотрено расторжение трудового договора в случае разглашения работником персональных данных, ставших известными работнику в связи с исполнением им трудовых обязанностей.

Виды дисциплинарных взысканий, порядок их применения и снятия устанавливаются главой 30 Трудового кодекса Российской Федерации от 20 декабря 2001г. № 197-ФЗ РФ и правилами внутреннего трудового распорядка Организации.

2. Административная ответственность

К административной ответственности за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) могут привлекаться как сама Организация, так и конкретные работники, исполняющие соответствующие трудовые обязанности.

Лица, виновные в нарушении правил обработки персональных данных, могут привлекаться к административной ответственности по следующим основаниям, приведенным в таблице 1.

Таблица 1 – Административная ответственность

Статья КоАП РФ[1]	Вид нарушения	Субъект нарушения	Ответственность
ст. 13.11, ч.1	Обработка ПДн в случаях, не предусмотренных законодательством Российской Федерации в области ПДн, либо обработка ПДн, несовместимая с целями сбора ПДн (за исключением случаев, предусмотренных ч.2 ст.13.11), если эти действия не содержат уголовно наказуемого деяния	Гражданин	Предупреждение или наложение административного штрафа в размере от 1000 до 3000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 5000 до 10 000 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 30 000 до 50 000 рублей
ст. 13.11, ч.2	Обработка ПДн без согласия в письменной форме субъекта ПДн на обработку его ПДн в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области ПДн, если эти действия не содержат уголовно наказуемого деяния, либо обработка ПДн с нарушением установленных законодательством Российской Федерации в области ПДн требований к составу сведений, включаемых в согласие в письменной форме субъекта ПДн на обработку его ПДн	Гражданин	Наложение административного штрафа в размере от 3000 до 5000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 10 000 до 20 000 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 15 000 до 75 000 рублей
ст. 13.11, ч.3	Невыполнение оператором предусмотренной законодательством Российской Федерации в области ПДн обязанности по опубликованию или обеспечению иным образом	Гражданин	Предупреждение или наложение административного штрафа в размере от 700 до 1 500 рублей

[1] Кодекс Российской Федерации об административных правонарушениях от 31 декабря 2001 г. № 195-ФЗ

Статья КоАП РФ[2]	Вид нарушения	Субъект нарушения	Ответственность
	неограниченного доступа к документу, определяющему политику оператора в отношении обработки ПДн, или сведениям о реализуемых требованиях к защите ПДн	Должностное лицо	Наложение административного штрафа в размере от 3000 до 6000 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 15 000 до 30 000 рублей
ст. 13.11, ч.4	Невыполнение оператором предусмотренной законодательством Российской Федерации в области ПДн обязанности по предоставлению субъекту ПДн информации, касающейся обработки его ПДн	Гражданин	Предупреждение или наложение административного штрафа в размере от 1000 до 2000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 4000 до 6000 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 20 000 до 40 000 рублей
ст. 13.11, ч.5	Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области ПДн, требования субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн об уточнении ПДн, их блокировании или уничтожении в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки	Гражданин	Предупреждение или наложение административного штрафа в размере от 1000 до 2000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 4000 до 10 000 рублей;
		Юридическое лицо	Наложение административного штрафа в размере от 25 000 тысяч до 45 000 рублей
ст. 13.11, ч.6	Невыполнение оператором при обработке ПДн без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством Российской Федерации в области ПДн сохранность ПДн при хранении материальных носителей ПДн и исключающих НСД, если это повлекло неправомерный или случайный доступ к ПДн, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении ПДн, при отсутствии признаков уголовно наказуемого деяния	Гражданин	Наложение административного штрафа в размере в размере от 700 до 2000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 4000 до 10 000 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 25 000 тысяч до 50 000 рублей
ст. 13.11, ч.7	Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области ПДн обязанности по обезличиванию ПДн либо несоблюдение установленных требований или методов по обезличиванию ПДн	Должностное лицо	Предупреждение или наложение административного штрафа в размере от 3000 до 6000 рублей
ст. 13.12, ч. 6	Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за	Гражданин	Наложение административного штрафа в размере от 500 до 1000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 1000 до 2000 рублей

Статья КоАП РФ[2]	Вид нарушения	Субъект нарушения	Ответственность
	исключением случаев, предусмотренных частями 1, 2 и 5 ст. 13.12 КоАП	Юридическое лицо	Наложение административного штрафа в размере от 10 000 до 15 000 рублей
ст. 13.14	Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 КоАП	Гражданин	Наложение административного штрафа в размере от 500 до 1000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 4000 до 5000 рублей
ст. 19.4, ч. 1	Неповиновение законному распоряжению или требованию должностного лица органа, осуществляющего государственный надзор (контроль), муниципальный контроль	Гражданин	Предупреждение или наложение административного штрафа в размере от 500 до 1000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 2000 до 4000 рублей
ст. 19.5, ч. 1	Невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), муниципальный контроль, об устранении нарушений законодательства	Гражданин	Наложение административного штрафа в размере от 300 до 500 рублей
		Должностное лицо	Наложение административного штрафа в размере от 1000 до 2000 рублей или дисквалификация на срок до трех лет
		Юридическое лицо	Наложение административного штрафа в размере от 10 000 до 20 000 рублей
ст. 19.7	Непредставление или несвоевременное представление в государственный орган (должностному лицу), орган (должностному лицу), осуществляющий (осуществляющему) государственный контроль (надзор), муниципальный контроль, сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, либо представление в государственный орган (должностному лицу), орган (должностному лицу), осуществляющий (осуществляющему) государственный контроль (надзор), муниципальный контроль, таких сведений (информации) в неполном объеме или в искаженном виде, за исключением случаев, предусмотренных ст. 6.16, ч.2 ст.6.31, ч.. 1, 2 и 4 ст. 8.28.1, ст.8.32.1, ч.5 ст.14.5, ч.2 ст.6.31, ч.4 ст.14.28, ч.1 ст.14.46.2, ст.19.7.1, 19.7.2, 19.7.2-1, 19.7.3, 19.7.5, 19.7.5-1, 19.7.5-2, 19.7.7, 19.7.8, 19.7.9, 19.7.12, 19.7.13, 19.7.14, 19.8, 19.8.3 КоАП	Гражданин	Предупреждение или наложение административного штрафа в размере от 100 до 300 рублей
		Должностное лицо	Наложение административного штрафа в размере от 300 до 500 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 3000 до 5000 рублей

3. Уголовная ответственность

Уголовная ответственность за нарушение правил работы с ПДн может наступить в случаях, указанных в таблице 2.

Таблица 2– Уголовная ответственность

Статья УК РФ	Вид нарушения	Ответственность
ст. 137, ч. 1	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации	Штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок до 360 часов, либо исправительными работами на срок до 1 года, либо принудительными работами на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо арестом на срок до 4 месяцев, либо лишением свободы на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет
ст. 137, ч. 2	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, совершенные лицом с использованием своего служебного положения	Штраф в размере от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 2 лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, либо принудительными работами на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового, либо арестом на срок до 6 месяцев, либо лишением свободы на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет
ст. 137, ч. 3	Незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия	Штраф в размере от 150 000 до 350 000 рублей или в размере заработной платы или иного дохода осужденного за период от 18 месяцев до 3 лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 3 до 5 лет, либо принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет или без такового, либо арестом на срок до 6 месяцев, либо лишением свободы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет
ст. 272, ч. 1	Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации	Штраф в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо исправительными работами на срок до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на тот же срок
ст. 272, ч. 2	Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб или совершенное из корыстной заинтересованности	Штраф в размере от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 2 лет, либо исправительными работами на срок от 1 года до 2 лет, либо ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 4 лет, либо лишением свободы на тот же срок
ст. 272, ч. 3	Деяния, предусмотренные ч.1-2 ст. 272 УК РФ, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного	Штраф в размере до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо ограничением

Статья УК РФ	Вид нарушения	Ответственность
	положения	свободы на срок до 4 лет, либо принудительными работами на срок до 5 лет, либо лишением свободы на тот же срок
ст. 272, ч. 4	Деяния, предусмотренные ч. 1-3 ст. 272 УК РФ, если они повлекли тяжкие последствия или создали угрозу их наступления	Лишение свободы на срок до семи лет
ст. 273, ч. 1	Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации	Ограничение свободы на срок до 4 лет, либо принудительные работы на срок до 4 лет, либо лишение свободы на тот же срок со штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев
ст. 273, ч. 2	Деяния, предусмотренные ч. 1 ст. 273, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности	Ограничение свободы на срок до 4 лет, либо принудительные работы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо лишением свободы на срок до 5 лет со штрафом в размере от 100 000 до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период от 2 до 3 лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового
ст. 273, ч. 3	Деяния, ч. 1-2 ст. 273, если они повлекли тяжкие последствия или создали угрозу их наступления	Лишение свободы на срок до семи лет
ст. 274, ч. 1	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб	Штраф в размере до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо исправительными работами на срок от 6 месяцев до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на тот же срок
ст. 274, ч. 2	Деяние, предусмотренное ч.1 ст. 274, если оно повлекло тяжкие последствия или создало угрозу их наступления	Принудительные работы на срок до 5 лет либо лишением свободы на тот же срок

4.Гражданско-правовая ответственность

Порядок защиты нематериальных благ, к числу которых относятся честь и доброе имя, деловая репутация; неприкосновенность частной жизни; личная и семейная тайна определяется Гражданским кодексом Российской Федерации и иными законами.

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

Руководителю ГБУЗ «ДКЦ № 1 ДЗМ»

_____;
(фамилия, имя и отчество субъекта персональных данных)

паспорт _____,
(серия и номер паспорта)

_____
(кем и когда выдан паспорт)

Адрес регистрации по месту жительства

_____

Согласие на передачу персональных данных

Настоящим, своей волей и в своем интересе, в соответствии со статьей 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» выражаю(даю) свое согласие [*Наименование Организации*] (юридический адрес: _____) на передачу [*Наименование учреждения*] (юридический адрес: _____) с использованием средств автоматизации с целью формирования внутренних информационных систем, ресурсов, справочников, баз данных, которые являются общедоступными источниками персональных данных, своих персональных данных:

- фамилия, имя, отчество;
- фотографическое изображение;
- дата рождения;
- рабочие номера телефонов и адрес электронной почты;
- номера мобильных телефонов;
- сведения о должности, подразделении, периоды отпусков (отсутствия).

Настоящее согласие предоставляется на срок действия трудового договора (*для органа исполнительной власти указать: служебного контракта государственного гражданского служащего*) и может быть отозвано в соответствии с частью 2 статьи 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» на основании письменного заявления в произвольной форме.

Условия настоящего Согласия мной лично прочитаны и мне понятны.

_____,
собственноручно указывается СОГЛАСЕН (СОГЛАСНА)

_____,
собственноручно **полностью** указывается фамилия, имя, отчество (если имеется)

_____ Дата:_____ _____20__г.
подпись

Утверждено приказом по
ГБУЗ «ДКЦ № 1 ДЗМ»
№ 530 от 15.09.2021 г.

Положение
о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

1. Общие положения

1.1. Положение об организации и проведении работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных (далее - Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Приказом ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", Приказом ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн).

1.2. Положение определяет порядок работы персонала в ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн согласно приложению № 7 к Положению, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в помещения ограниченного доступа.

2. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн

Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа и в соответствии со списком лиц, допущенных к работе в ИСПДн. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн, назначается ответственный за выполнение работ по обеспечению безопасности ПДн при их обработке в ИСПДн (администратор безопасности); с целью контроля выполнения необходимых мероприятий по обеспечению безопасности - ответственный за организацию обработки ПДн.

2.2. Пользователь имеет право решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей согласно приложению № 2 к Положению.

2.3. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

2.4. Вход пользователя в систему может осуществляться по персональному логину паролю.

2.5. Запись информации, содержащей ПДн, осуществляется пользователем на съемные машинные носители информации, соответствующим образом учтенные в Журнале учета машинных носителей согласно приложению № 2 к Положению.

2.6. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

2.7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн; - знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;

- хранить в тайне свой пароль (пароли) (в соответствии с пунктами 8.5, 8.6 данного Положения и с установленной периодичностью менять свой пароль (пароли));

- выполнять требования Положения по организации антивирусной защиты в полном объеме.

Немедленно известить ответственного за эксплуатацию ИСПДн либо ответственного за выполнение работ по обеспечению безопасности персональных данных в случае компрометации личных паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данным, защищаемым СВТ;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на компьютеры технических средств защиты;

- непредусмотренных отводов кабелей и подключенных устройств.

Пользователю категорически запрещается: - использовать компоненты программного и аппаратного обеспечения СВТ в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.

2.8. Ответственный за выполнение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - Администратор безопасности) обязан:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС), установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;

- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

- вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;

- своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

- контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;

- проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;

- вести журналы согласно приложениям № 1, № 2, № 3, № 4, № 5, № 6, № 7, № 8, № 9, № 10 к Положению;

- контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;

- обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;

- вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале согласно приложению № 10 к Положению;

- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в 10 дней;

- организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации. Сопровождать подсистемы обеспечения целостности информации в ИСПДн;

- периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей; - восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

- вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;

- контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;

- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядка и правил проведения антивирусного тестирования:

- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

- сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИСПДн;

- контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;

- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);

- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

- вести Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания СВТ согласно приложению № 5 к Положению, выполнения профилактических работ, установки и модификации аппаратных и программных средств СВТ;

- поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения, в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

- докладывать ответственному за защиту информации, ответственному за эксплуатацию ИСПДн о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

2.9. Администратор безопасности, а также ответственный за организацию обработки персональных данных имеют право:

- требовать от сотрудников - пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

- инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;

- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации и порядок реагирования на внештатные ситуации

3.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

3.2. К использованию для создания резервной копии в ИСПДн допускаются только зарегистрированные в журнале учета носители.

3.3. Администратор безопасности ежеквартально осуществляет резервное копирование конфиденциальной информации.

3.4. Носители информации (ЖМД, CD, USB-накопитель, другие), предназначенные для создания резервной копии и хранения конфиденциальной

информации, выдаются установленным порядком руководителем, ответственным за защиту информации, и (или) администратором. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности или руководителю, или ответственному за защиту информации.

3.5. Перед резервным копированием пользователь или администратор безопасности обязан проверить электронный носитель (ЖМД, CD, USB-накопитель) на отсутствие вирусов.

3.6. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль в соответствии с разделом 7 настоящего Положения.

3.7. Запрещается запись посторонней информации на электронные носители (ЖМД, CD, USB-накопитель и другие) резервной копии.

3.8. Порядок создания резервной копии:

- вставить в компьютер зарегистрированный электронный носитель (ЖМД, CD, USB-накопитель, другие) для резервного копирования;
- выбрать необходимый каталог (файл) для создания резервного архива;
- при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;
- выполнить процедуру создания резервной копии;
- произвести копирование на отчуждаемый носитель;
- произвести отключение отчуждаемого носителя и, создав необходимые записи в журналах, убрать носитель в хранилище, указанного в журнале учета хранилищ, согласно приложению № 3 к Положению.

3.9. Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище совместно с ключевой и аутентифицирующей информацией.

3.10. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

3.11. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

3.12. При необходимости ремонта технических средств с них удаляются опечатывающие пломбы и по согласованию с администратором безопасности, ответственным за защиту информации, при условии проведенной аттестации информационной системы, представителем организации, проводившей аттестацию, оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

3.13. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

3.14. При восстановлении работоспособности средств защиты информации следует выполнить их настройку.

3.15. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

3.16. Ответственность за проведение резервного копирования в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора безопасности.

3.17. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора безопасности.

3.18. Ответственность за проведение мероприятий по восстановлению средств защиты информации (далее - СЗИ) возлагается на администратора безопасности.

3.19 Нештатными ситуациями является:

- разглашение информации ограниченного доступа сотрудниками ГБУЗ «ДКЦ № 1 ДЗМ» имеющими к ней право доступа, в том числе:
  - разглашение информации лицам, не имеющим права доступа к защищаемой информации;
  - передача информации по незащищенным каналам связи;
  - обработка информации на незащищенных технических средствах обработки информации;
  - опубликование информации в открытой печати и других средствах массовой информации;
  - передача носителя информации лицу, не имеющему права доступа к ней;
  - утрата носителя с информацией.
- неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
  - несанкционированное изменение информации;
  - несанкционированное копирование информации;
- несанкционированный доступ к защищаемой информации:
  - несанкционированное подключение технических средств к средствам и системам ИСПДн;
  - использование закладочных устройств;
  - использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ИСПДн;
  - использование злоумышленником уязвимостей программного обеспечения ИСПДн;
  - использование злоумышленником программных закладок;
  - заражение ИСПДн злоумышленником программными вирусами;
  - хищение носителей информации;
  - нарушение функционирования технических средств обработки информации;
  - блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
- дефекты, сбои, отказы, аварии технических средств и систем ИСПДн;
- дефекты, сбои, отказы программного обеспечения ИСПДн;
- сбои, отказы и аварии систем обеспечения ИСПДн;
- природные явления, стихийные бедствия:
  - термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
  - механические факторы (повреждения зданий, землетрясения и т. д.);
  - электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

3.20. В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей политикой, администратором безопасности и группой по реагированию на инциденты информационной безопасности (далее – ГРИИБ) вырабатывается конкретный план действий с учетом текущей ситуации.

3.21 Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 11 настоящей Политики.

3.22. С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления по результатам тренировок изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.

3.23. Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

3.24. В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

- корректное отключение технических средств ИСПДн до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
- предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ИСПДн а также меры по замене/ремонту вышедших из строя средств и систем;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

3.25. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями выполняются следующие действия:

- Пользователи корректно отключают и обесточивают свои рабочие места;
- системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;
- Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;
- в случае нарушения корректной работы технических средств в ГИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;
- в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.

4. Порядок контроля защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий

4.1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение

характеристик безопасности информации или работоспособности систем информатизации.

4.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в подразделениях, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

- выявление демаскирующих признаков объектов ИСПДн;

- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

4.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн, и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

4.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных (далее - ОБ ПДн);

- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;

- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

- эффективность применения организационных и технических мероприятий по защите информации;

- устранение ранее выявленных недостатков.

Кроме того, могут проводиться необходимые измерения и расчеты приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии ФСТЭК России.

4.5. Основными видами технического контроля являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

4.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор безопасности докладывает руководителю для принятия ими решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

4.7. Невыполнение предписанных мероприятий по защите ПДн считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию главного врача или ответственного за организацию обработки персональных данных проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора безопасности. Комиссия обязана установить, имела ли место утечка сведений, обстоятельства, ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования руководитель принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

4.8. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, как правило, силами администратора безопасности и (или) ответственного за защиту информации, в соответствии с утвержденным планом или по согласованию с руководителем.

4.9. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора безопасности, ответственного за защиту информации, ответственного за эксплуатацию объекта. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

4.10. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в Аттестате соответствия (если проводилась аттестация), и (или) требованиям по безопасности персональных данных.

4.11. В ходе обследования проверяется:

- соответствие текущих условий функционирования обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;
- соблюдение организационно-технических требований помещений, в которых располагается ИСПДн;
- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;
- соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в настоящем Положении;
- выполнение требований по защите информационных систем от несанкционированного доступа;
- выполнение требований по антивирусной защите.

4.12. Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в выделенных и защищаемых помещениях, а также других нарушений и способов возникновения каналов утечки информации необходимо:

- тщательно осмотреть мебель, сувениры (особенно иностранного производства), оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы;
- вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;
- проверить качество установки стеклопакетов оконных проемов;
- провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры), при необходимости для проведения данных видов работ могут привлекаться организации, имеющие соответствующие лицензии ФСБ России.

5. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных

5.1. Перед началом работы в ИСПДн пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации под роспись.

5.2. Пользователи должны продемонстрировать администратору безопасности и (или) ответственному за защиту информации наличие необходимых знаний и умений для выполнения требований настоящего Положения. Администратор безопасности должен вести журнал учета проверок знаний и навыков пользователей согласно приложению № 8 к Положению.

5.3. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего Положения, к работе в ИСПДн не допускаются.

5.4. Ответственным за организацию обучения и оказание методической помощи является администратор безопасности.

5.5. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИСПДн, организаций-лицензиатов ФСТЭК России и ФСБ России.

5.6. К работе в ИСПДн допускаются только сотрудники, прошедшие первичный инструктаж ОБ в ИСПДн и показавшие твердые теоретические знания и практические навыки, о чем делается соответствующая запись в Журнале учета допуска к работе в ИСПДн согласно приложению № 6 к Положению.

6. Порядок проверки электронного журнала обращений к ИСПДн

6.1. Настоящий раздел Положения определяет порядок проверки электронных журналов обращений к ресурсам ИСПДн.

6.2. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к защищаемой информации в ИСПДн.

6.3. Право проверки электронного журнала обращений имеют:

- ответственный за организацию обработки персональных данных;
- ответственный за выполнение работ по обеспечению безопасности ПДн при их обработке в ИСПДн;
- главный врач.

6.4. На технических средствах ИСПДн, на которых установлены специализированные средства защиты информации (далее - СЗИ), проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

6.5. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлены случай НСД к информации конфиденциального характера, то проводится расследование согласно пункту 4.7 данного Положения.

6.6. Проверке подлежат все электронные журналы ИСПДн.

6.7. Проверка должна проводиться не реже чем один раз в неделю с целью своевременного выявления фактов нарушения требований настоящего Положения.

6.8. Факты проверок электронных журналов отражаются в специальном журнале проверок. После каждой проверки Администратор безопасности делает соответствующую отметку в журнале и ставит свою роспись.

7. Правила антивирусной защиты

7.1. Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения (ПО), компьютерных вирусов и устанавливают ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение. Настоящие правила распространяются на все объекты ИСПДн.

7.2. К использованию на компьютерах допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

7.3. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности.

7.4. Администратор безопасности осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

7.5. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

7.6. Еженедельно в начале работы после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Настройки средств антивирусной защиты должны быть выполнены в соответствии с требованиями безопасности персональных данных определенного для данной ИСПДн класса. Настройку средств антивирусной защиты выполняет администратор безопасности.

7.7. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

7.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера администратором безопасности должна быть выполнена антивирусная проверка ИСПДн.

7.9. На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

7.10. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

7.11. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на ответственного за защиту информации.

7.12. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

8. Правила парольной защиты

8.1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

8.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора безопасности.

8.3. Личные пароли должны генерироваться и распределяться централизованно:

- пароль должен быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущих;
- пользователь не имеет права сообщать личный пароль другим лицам:
- не хранить пароль на бумажном носителе
- не хранить пароль в заметках на телефоне

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

8.4. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств, технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение руководителю структурного подразделения. Запечатанные конверты (пеналы) с паролями исполнителей должны храниться в недоступном месте у руководителя структурного подразделения.

8.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.

8.6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий должна производиться администратором безопасности (либо новым постоянным пользователем) немедленно после окончания последнего сеанса работы данного пользователя с системой на основании указания начальника отдела.

8.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности.

8.8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.

8.9. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности.

9. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

9.1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

9.2. Все изменения конфигураций технических и программных средств ИСПДн должны производиться только на основании заявок ответственного за эксплуатацию конкретного ИСПДн.

9.3. Право внесения изменений в конфигурацию аппаратно-программных средств, защищенных ИСПДн предоставляется:

- в отношении системных и прикладных программных средств - администратору безопасности по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн;

- в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты - администратору безопасности по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн.

9.4. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме перечисленных в п. 9.3 уполномоченных сотрудников и подразделений, запрещено.

9.5. Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн инициируется заявкой ответственного за эксплуатацию ИСПДн.

9.6. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

- установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн);

- обновление (замена) на компьютере (ах) программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);

- удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

9.7. Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

9.8. Заявку ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает ответственный за организацию обработки персональных данных, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений, после чего заявка передается администратору безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке ИСПДн.

9.9. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн, тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах (обновление) и удаление системных и прикладных программных средств производится администратором безопасности по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

9.10. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

9.11. Установка и обновление ПО (системного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей; прикладного ПО - с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

9.12. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.

9.13. После установки (обновления) ПО администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки и

произвести соответствующую запись в Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн согласно приложению № 5 к Положению, делает отметку о выполнении (на обратной стороне заявки) и в Техническом паспорте.

9.14. Формат записей Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн устанавливается главным врачом.

9.15. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за эксплуатацию ИСПДн докладывает об этом ответственному за защиту информации, который в свою очередь связывается с сотрудниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкциям. В данном случае администратор безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИСПДн и Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн у ответственного за защиту информации.

9.16. Копии заявок могут храниться у администратора безопасности:

- для восстановления конфигурации ИСПДн после аварий;
- для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты ИСПДн.

9.17. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора безопасности и сотрудника, ответственного за эксплуатацию данной ИСПДн.

9.18. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном компьютере.

9.19. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя ("группового имени") запрещено.

9.20. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн, в которой указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);
- должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

9.21. Заявку рассматривает ответственный за организацию обработки персональных данных, визируя ее, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем подписывает задание администратору безопасности на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

9.22. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие

необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 360 дней.

9.23. После внесения изменений в списки пользователей администратор безопасности должен обеспечить настройки средств защиты, соответствующие требованиям безопасности указанной ИСПДн. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя - администратор безопасности.

9.24. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное(-ые) значение(-ия) пароля(-ей), которое(-ые) он обязан сменить при первом же входе в систему.

9.25. Исполненные заявка и задание (за подписью администратора безопасности) передаются руководителю на хранение, которые могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий ИСПДн;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;
- для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

10. Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических

10.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее - СЗИ).

10.2. Технические средства защиты информации являются важным компонентом ОБ ПДн.

10.3. Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками, обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

10.4. Право проверки соблюдения условий использования средств защиты информации имеют:

- главный врач;
- ответственный за организацию обработки персональных данных;
- ответственный за выполнение работ по обеспечению безопасности персональных данных.

10.5. Пользователю ИСПДн категорически запрещается:

- обрабатывать конфиденциальную информацию с отключенными СЗИ;
- менять настройки СЗИ.

10.6. Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ, предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

10.7. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлено нарушение требования п. 10.5, то проводится расследование согласно пункту 4.7 данного Положения.

10.8. Криптографические СЗИ должны использоваться в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими.

11. Порядок охраны и допуска посторонних лиц в защищаемые помещения

11.1. Настоящее Положение устанавливает порядок охраны защищаемых помещений ИСПДн.

11.2. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.Список сотрудников, имеющих право вскрывать помещения, утверждается главным врачом.

11.3. При отсутствии сотрудников, ответственных за вскрытие помещений, данные помещения могут быть вскрыты комиссией, созданной на основании распоряжения, о чем составляется акт.

11.4. При закрытии помещений сотрудники, ответственные за помещения, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации, на которых содержится конфиденциальная информация, убираются для хранения в опечатываемый сейф (металлический шкаф).

11.5. Руководитель, ответственный за защиту информации, и администратор безопасности организуют проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

Если обнаружено вторжение в защищаемое помещение, то необходимо действовать в порядке, указанном в пункте 4.7 настоящего Положения.

11.6. В соответствии с требованиями данного Положения при обработке защищаемой информации в ИСПДн исключить неконтролируемое пребывание посторонних лиц в пределах границ контролируемой зоны ИСПДн, определенных соответствующим приказом.

12. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации

12.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускаются стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим Порядком.

12.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).

12.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирания информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны исключать возможность восстановления информации.

12.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

12.5. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

12.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию ИСПДн, ответственный за защиту информации, администратор безопасности.

12.7. Правила и процедуры восстановления ИСПДн при возникновении нештатных ситуаций.

13. Заключительные положения

13.1. Требования настоящего Положения обязательны для всех сотрудников, обрабатывающих конфиденциальную информацию (персональные данные).

13.2. Нарушение требований настоящего Положения влечет за собой ответственность в соответствии с законодательством Российской Федерации.

Приложение 1 к Положению

Журнал
поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов

	Наименование криптосредства эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение 2 к Положению

Журнал
учета машинных носителей информации

N п/п	Регистрационный (учетный) номер носителя	Вид носителя	Тип носителя и его емкость	Дата поступления	Расписка в получении (Ф.И.О., подпись, дата)	Расписка в обратном приеме (Ф.И.О., подпись, дата)	Место хранения	Дата и номер акта об уничтожении	Примечание
1	2	3	4	5	6	7	8	9	10

Приложение 3 к Положению

Журнал
учета хранилищ

N п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатации	Примечание
	2	3	4	5	6	7	8

Приложение 4 к Положению

Журнал
периодического тестирования средств защиты информации

N п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответственного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования
	2	3	4	5	6	7	8

Приложение 5 к Положению

Журнал
учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн

N п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	Ф.И.О. исполнителей и их подписи	Ф.И.О. ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)
1	2	3	4	5	6	7

Приложение 6 к Положению

Журнал
учета пользователей, допущенных к информационным системам персональных данных

N п/п	Дата	Фамилия, имя, отчество пользователя	Наименование ИСПДн	Подпись пользователя об ознакомлении с Положением и требованиями по безопасности	Подпись администратора безопасности о готовности пользователя к работе в ИСПДн	Примечание
1	2	3	4	5	6	7

Приложение 7 к Положению

Журнал
проверок электронных журналов

N п/п	Дата проверки	Наименование ИСПДн, компьютера, технического средства	Наименование проверяемого журнала	Выявленные нарушения требований безопасности, нештатные ситуации	Подпись администратора безопасности	Примечание
1	2	3	4	5	6	7

Приложение 8 к Положению

Журнал
проверок знаний и навыков пользователей

N п/п	Ф.И.О. должность, пользователя	Дата проведения проверки	Подпись пользователя	Отметка о результатах проведения проверок	Подпись администратора безопасности	Примечание
1	2	3	7	8	9	10

Приложение 9 к Положению

Журнал
регистрации письменных запросов

№ п/п	Вх. N письма	Дата получения запроса	Ф.И.О. гражданина	Сведения о документе, удостоверяющем личность			Отметка о предоставлении доступа к ПДн (отказе в доступе)	Исх. номер и дата письма с ответом на запрос	Ф.И.О., должность, роспись сотрудника, выдавшего ответ	Примечание
				Номер, серия	Дата выдачи	Кем выдан				
1	2	3	4	5	6	7	8	9	10	11

Приложение 10 к Положению

Журнал
регистрации ПДн

N п/п	Исх. N пакета	Дата отправки	Ф.И.О. ответственного сотрудника	Сведения о передаваемых ПДн			Наименование организации получателя	Вх. N пакета	Ф.И.О., должность, роспись сотрудника, принявшего пакет	Примечание
				Количество уникальных записей	Категория ПДн	Цель передачи				
1	2	3	4	5	6	7	8	9	10	11

Приложение № 11

План обеспечения непрерывности функционирования ИСПДн

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
1.	Разглашение защищаемой информации сотрудниками, имеющими легальные права доступа к ней		Администратору безопасности сразу после обнаружения инцидента	1 час	1 день
2.	Обнаружение несанкционированного скопированной или измененной конфиденциальной информации		Администратору безопасности сразу после обнаружения инцидента	1 час	1 день
3.	Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней		Администратору безопасности сразу после обнаружения инцидента	Сразу после получения информации об инциденте	1 день
4.	Обнаружение подключения технических средств к средствам и системам объекта информатизации		Администратору безопасности сразу после обнаружения инцидента	1 час	3 часа

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
5.	Подключение технических средств к средствам и системам ИСПДн в текущий момент времени		Администратору безопасности сразу после обнаружения инцидента	Сразу после получения информации об инциденте	3 часа
6.	Обнаружение закладочных устройств		Администратору безопасности сразу после обнаружения инцидента	Сразу после получения информации об инциденте	1 день
7.	Установка закладочных устройств злоумышленником в текущий момент времени		Администратору безопасности сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
8.	Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени		Администратору безопасности сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
9.	Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки		Администратору безопасности сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
10.	Использование дефектов программного обеспечения ОИ		Администратору безопасности сразу после	10 минут в рабочее время	12 часов

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
	внешним нарушителем в текущий момент времени		обнаружения инцидента	(1 час в нерабочее)	
11.	Использование программных закладок внешним нарушителем в текущий момент времени		Администратору безопасности сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
12.	Использование программных закладок внутренним злоумышленником или обнаружение факта использования		Администратору безопасности сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
13.	Обнаружение программных вирусов		Администратору безопасности сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
14.	Хищение носителя защищаемой информации		Администратору безопасности сразу после обнаружения инцидента	1 сутки	3 дня
15.	Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Нарушена работа одного пользователя	Администратору безопасности сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
16.	Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
17.	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени		Администратору сразу после обнаружения инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день
18.	Обнаружение произошедшего факта блокировки доступа к защищаемой информации		Администратору сразу после обнаружения инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день
19.	Ошибки пользователей системы при эксплуатации ТС, программных		Администратору сразу после	2 часа в рабочее время	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
	средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации		обнаружения инцидента	(12 часов в нерабочее)	
20.	Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	20 минут	1 день
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	20 минут	2 дня
21.	Дефекты, сбои, отказы, аварии ТС, программных средств и ИСПДн	Сбой ТС и систем ИСПДн	Администратору сразу после обнаружения инцидента	1 час	2 дня
		Отказ ТС и систем ИСПДн, затронувший работу группы пользователей	Администратору сразу после обнаружения инцидента	1 час в рабочее время (8 часов в нерабочее)	1 день
		Отказ ТС и систем ИСПДн, затронувший	Администратору сразу после обнаружения инцидента	1 час	2 дня

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
		работу одного пользователя			
		Авария ТС и систем ИСПДн	Администратору сразу после обнаружения инцидента	1 час	1 день
22.	Сбои, отказы и аварии систем обеспечения ГИС	Сбой систем обеспечения ИСПДн	Ответственному за материально-техническое обеспечение сразу после инцидента	1 час	1 день
		Отказ систем обеспечения ИСПДн, затронувший работу группы пользователей	Ответственному за материально-техническое обеспечение и Администратору сразу после обнаружения инцидента	1 час	1 день
		Отказ систем обеспечения ИСПДн, затронувший работу одного пользователя	Ответственному за материально-техническое обеспечение сразу после инцидента	1 час	2 дня

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
		Авария систем обеспечения ИСПДн	Ответственному за материально-техническое обеспечение, Администратору сразу после обнаружения инцидента	1 час	1 день
23.	Природные явления, стихийные бедствия, несущие угрозу жизни человека		Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации	10 минут	30 минут
24.	Природные явления, стихийные бедствия, не несущие угрозу жизни человека		Руководителю, заместителям Руководителя, Администратору	10 минут	1 час