«УТВЕРЖДАЮ»
Главный врач ГАУЗ РК
«стоматологическая поликлиника
г.Феодосии»
_____ Ю.В. Кирик
«13» 01 2015 г.

ПОЛОЖЕНИЕ

по организации и проведению работ по обеспечению безопасности персональных данных

Определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств. Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных. Неавтоматизированная обработка персональных данных - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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

передачу), обезличивание, блокирование, уничтожение персональных данных. Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности. Оператор (персональных данных) - государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъек-ту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Раскрытие персональных данных - умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной

жизни субъекта персональных данных.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация. Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Сокращения

ИСПДн	информационная система персональных данных
ПДн	персональные данные
ДСП	для служебного пользования

1 **Введение**

1.1. Настоящее Положение имеет своей целью закрепление механизмов обеспечения прав субъектов ПДн на сохранение конфиденциальности информации о фактах, событиях и обстоятельствах их жизни.

1.2. Настоящее Положение определяет порядок работы (получения, обработки, использования, хранения и т.д.) с ПДн.

1.3. Положение по организации и проведению работ по обеспечению безопасности ПДн в Автономном учреждение здравоохранения «Республиканская стоматологическая поликлиника» (далее- Организация) разработано на основе анализа требований действующего законодательства Российской Федерации и нормативных документов, регламентирующих вопросы защиты ПДн, с учетом современного состояния и стратегии развития информационных технологий.

2 **Понятие и состав персональных данных**

Под ПДн понимается информация, необходимая Организации в связи с трудовыми отношениями и касающаяся конкретного субъекта ПДн, его родственников, а также сведения о фактах, событиях и обстоятельствах жизни субъекта ПДн, позволяющие идентифицировать его личность и личность его родственников. К ПДн относятся следующие сведения и документы:

- все биометрические данные о субъекте ПДн;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- место жительства (пребывания);
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора;
- содержание налоговых деклараций;
- личные дела, личные карточки и трудовые книжки;
- копии отчетов, направляемые в органы статистики;
- анкеты, заполняемые субъектом ПДн;
- копии документов об образовании;
- результаты медицинского обследования.

3 **Принципы обработки персональных данных**

3.1. Обработка ПДн должна осуществляться на основе принципов:

– законности целей и способов обработки ПДн и добросовестности; соответствия целей обработки ПДн целям, заранее определенным и

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

3.2. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.3. Субъект ПДн является собственником своих ПДн и самостоятельно решает вопрос передачи Организации своих ПДн.

3.4. Держателем ПДн является Организация, которой субъект ПДн добровольно передает во владение свои ПДн. Она выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в *• пределах, установленных законодательством.

3.5. Право доступа к ПДн субъекта ПДн имеют лица, уполномоченные Организацией.

3.6. Потребителями (пользователями) ПДн являются юридические и физические лица, обращающиеся к собственнику или держателю ПДн за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

3.7. Получение, хранение, комбинирование, передача или любое другое использование ПДн субъекта ПДн может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативно-правовых актов, содействия субъектам ПДн в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности субъектов ПДн, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

4 Обработка и хранение персональных данных

4.1. Условием обработки ПДн субъекта ПДн является его письменное согласие (Приложение № 5). Субъект ПДн принимает решение о предоставлении своих ПДн и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных п. 4.2 настоящего Положения. Согласие на обработку ПДн может быть отозвано субъектом ПДн.

4.2. Согласие субъекта ПДн на обработку его ПДн не требуется в следующих случаях:

1) обработка ПДн осуществляется на основании федерального закона, устанавливающего ее цель, условия получения ПДн и круг субъектов ПДн, ПДн, которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка ПДн осуществляется в целях исполнения трудового или иного

договора или соглашения между субъектом ПДн и Организацией;
3) обработка ПДн осуществляется для статистических или иных научных целей при условии обязательного обезличивания ПДн;
4) обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение его согласия при данных обстоятельствах невозможно;
5) обработка ПДн необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;
6) обработка ПДн осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта ПДн;
7) обработка ПДн, подлежащих опубликованию в соответствии с федеральными законами, в том числе ПДн лиц, замещающих государственные должности, должности государственной гражданской службы, ПДн кандидатов на выборные государственные или муниципальные должности.

4.3. Письменное согласие субъекта ПДн на обработку его ПДн должно включать в себя:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес Организации, получающего согласие субъекта ПДн;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта ПДн;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Организацией способов обработки ПДн;
- срок, в течение которого действует согласие, а также порядок его отзыва.

В случае недееспособности субъекта ПДн согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта ПДн.

В случае смерти субъекта ПДн согласие на обработку его ПДн при необходимости дает в письменной форме один из его наследников, если такое согласие не было дано работником при его жизни.

4.4. Не допускается получение и обработка ПДн субъекта ПДн о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных п. 4.5 настоящего Положения.

4.5. Обработка указанных в п. 4.4. настоящего положения ПДн допускается в случаях, если:

1) субъект ПДн дал согласие в письменной форме на обработку своих ГЩн;

2) ПДн являются общедоступными;
3) ПДн относятся к состоянию здоровья субъекта ПДн, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта ПДн в данный момент невозможно;
4) обработка ПДн осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка ПДн осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
5) обработка ПДн необходима в связи с осуществлением правосудия;
6) обработка ПДн осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

4.6. Обработка ПДн о судимости может осуществляться в соответствии с федеральными законами.

4.7. Обработка ПДн, перечисленных в п. 4.4. настоящего положения должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

4.8. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические ПДн), могут обрабатываться только при наличии согласия субъекта ПДн в письменной форме, за исключением случаев, предусмотренных п. 4.9 настоящего положения.

4.9. Обработка биометрических ПДн может осуществляться без согласия субъекта ПДн в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, уголовно-исполнительным законодательством Российской Федерации.

4.10. Документы, содержащие ПДн субъекта ПДн, составляют его личное дело. Личное дело хранится уполномоченным лицом на бумажных носителях, а помимо этого может храниться в виде электронных документов. Личное дело пополняется на протяжении всей трудовой деятельности субъекта ПДн. Письменные доказательства получения Организацией согласия субъекта ПДн на обработку его ПДн хранятся в личном деле субъекта ПДн.

4.11. Документы и внешние электронные носители информации, содержащие ПДн, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

5 Организация разрешительной системы доступа пользователей к обрабатываемой в информационной системе персональных данных информации

6

5.1 Требования при регистрации субъекта персональных данных

5.1.1 Оператор получает сведения о ПДн субъекта ПДн из следующих документов:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета;
- документ об образовании, о квалификации или наличии специальных знаний;
- анкета, заполняемая субъектом ПДн при приеме на работу;
- иные документы и сведения, предоставляемые субъектом ПДн при приеме на работу и в процессе работы.

5.1.2. Все ПДн субъекта ПДн получаются у него самого. Сотрудник, ответственный за документационное обеспечение кадровой деятельности, принимает от субъекта ПДн документы, проверяет их полноту и правильность указываемых сведений.

Если ПДн субъекта ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (Приложение № 3). Оператор должен сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа субъекта ПДн дать письменное согласие на их получение (Приложение № 4).

5.2 Порядок предоставления доступа к информационным ресурсам информационной системы персональных данных

Внутренний доступ к ПДн субъекта ПДн имеют сотрудники структурных подразделений Организации, которым эти данные необходимы для выполнения должностных обязанностей.

6. Конфиденциальность персональных данных

6.1. Оператором и третьими лицами, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных п. 6.2 настоящего положения.

6.2. Обеспечение конфиденциальности ПДн не требуется:

- . в случае обезличивания ПДн;
- в отношении общедоступных ПДн

7 Общедоступные источники ПДн

7.1. В целях информационного обеспечения деятельности могут создаваться общедоступные источники ПДн (в том числе справочники, адресные книги и др.). В общедоступные источники ПДн с письменного

согласия субъекта ПДн (Приложение № 6) могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн, предоставленные субъектом ПДн.

7.2. Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников ПДн по его требованию либо по решению Организации, либо суда или иных уполномоченных государственных органов.

8 Права и обязанности сторон при работе с персональными данными

8.1. Субъект ПДн **обязан:**

- передавать Оператору или его представителю комплекс достоверных, документированных ПДн, состав которых установлен трудовым законодательством, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и др.
- своевременно сообщать Организации об изменении своих ПДн.

8.2. Субъект ПДн имеет **право:**

- получать полную информацию о своих ПДн;
- иметь свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей его ПДн, за исключением случаев, предусмотренных действующим законодательством;
- иметь доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;
- получать сведения об Организации, о месте его нахождения, о наличии у Организации ПДн, относящихся к соответствующему субъекту ПДн;
- требовать от Организации уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- получать информацию, касающуюся обработки его ПДн, в том числе содержащую: подтверждение факта обработки ПДн Организацией, а также цель такой обработки; способы обработки ПДн, применяемые Организацией; сведения о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ; перечень обрабатываемых ПДн и источник их получения; сроки обработки ПДн, в том числе сроки их хранения; сведения о том, какие юридические последствия для него может повлечь за собой обработка его ПДн;
- при отказе Организации исключить или исправить ПДн субъекта ПДн он имеет право заявить в письменной форме Организации о своем несогласии с соответствующим обоснованием такого несогласия.

Сведения о наличии ПДн должны быть предоставлены субъекту ПДн в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн. Доступ к своим ПДн предоставляется субъекту или его законному представителю Организацией при личном обращении либо при получении запроса (Приложение № 7). Запрос должен содержать номер основного документа, удостоверяющего личность субъекта или его законного

представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

8.3. Право субъекта ПДн на доступ к своим ПДн ограничивается в случае, если:

1) обработка ПДн, в том числе ПДн, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка ПДн осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;

3) предоставление ПДн нарушает конституционные права и свободы других лиц.

8.4. Запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных п. 8.5 настоящего положения.

8.5. Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн только при наличии согласия субъекта в письменной форме (Приложение № 5) или в случаях, предусмотренных федеральными законами.

8.6. Организация обязана разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов (Приложение № 4). Организация обязана рассмотреть возражение субъекта в течение семи рабочих дней со дня его получения и уведомить его о результатах рассмотрения такого возражения.

8.7. Если обязанность предоставления ПДн субъектом ПДн установлена федеральным законом, оператор обязан разъяснить субъекту ПДн юридические последствия отказа предоставить свои ПДн.

8.8. Если ПДн были получены не от субъекта ПДн, за исключением случаев, если ПДн были предоставлены Организации на основании федерального закона или если ПДн являются общедоступными, Организация до начала обработки таких ПДн обязан предоставить субъекту ПДн

следующую информацию (Приложение № 8):

1) наименование (фамилия, имя, отчество) и адрес Организации или его представителя;

2) цель обработки ПДн и ее правовое основание;

3) предполагаемые пользователи ПДн;

4) права субъекта.

8.9. Оператор обязан безвозмездно предоставить субъекту возможность ознакомления с ПДн, относящимися к соответствующему субъекту, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие ПДн по предоставлении субъектом сведений, подтверждающих, что ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях, уничтожении или блокировании и предпринятых мерах Организация обязана уведомить субъекта ПДн и третьих лиц, которым ПДн этого субъекта были переданы (Приложение № 9).

8.10. В случае выявления недостоверных ПДн или неправомерных действий, с ними Организация обязана осуществить блокирование ПДн, относящихся к соответствующему субъекту, с момента получения такой информации на период проверки. В случае подтверждения факта недостоверности ПДн Оператор на основании соответствующих документов обязан уточнить ПДн и снять их блокирование.

В случае выявления неправомерных действий с ПДн Организация в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Организация в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, обязан уничтожить ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Организация обязана уведомить субъекта ПДн (Приложение № 9).

8.11. В случае достижения цели обработки ПДн Организация обязана незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий трех рабочих дней с даты достижения цели обработки ПДн, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта (Приложение № 9).

8.12. В случае отзыва субъектом ПДн согласия на обработку своих ПДн Организация обязана прекратить обработку ПДн и уничтожить ПДн в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон. Об уничтожении ПДн Организация обязана уведомить субъекта ПДн (Приложение № 9).

9 **Доступ, передача и защита персональных данных**

9.1. Внутренний доступ к ПДн субъекта ПДн имеют уполномоченные сотрудники структурных подразделений Организации, которым эти данные необходимы для выполнения должностных обязанностей.

Для хранения ПДн используются специально оборудованные шкафы или

сейфы, которые запираются на ключ.

9.2. После увольнения субъекта документы, содержащие его ПДн, хранятся у Организации в течение сроков, установленных архивным законодательством.

9.3. Внешний доступ со стороны третьих лиц к ПДн субъекта ПДн осуществляется только с письменного согласия субъекта ПДн, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью субъекта ПДн или других лиц, и иных случаев, установленных законодательством.

9.4. Организация обязана сообщать ПДн субъекта ПДн по надлежаще оформленным запросам суда, прокуратуры, правоохранительных органов.

9.5. При передаче ПДн субъекта ПДн Организация должна соблюдать следующие требования:

9.5.1. Передача внешнему потребителю:

- передача ПДн от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;
- ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения Организации и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений;
- не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу;
- сведения передаются в письменной форме и должны иметь гриф конфиденциальности.

9.5.2. Передача внутреннему потребителю:

- Оператор вправе разрешать доступ к ПДн субъектов ПДн только специально уполномоченным лицам;
- потребители ПДн должны подписать обязательство о неразглашении ПДн субъектов (Приложение № 2).

9.6. Схема разделения полномочий и зон ответственности.

9.6.1. **«Внутренняя защита»**

Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителем и специалистами Организации. Для обеспечения безопасности ПДн субъектов ПДн Организация **обязана** соблюдать следующие правила:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей ПДн;
- избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;

- знание сотрудниками требований нормативно-методических документов по обеспечению безопасности ПДн;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты сведений при работе с конфиденциальными документами.

9.6.2. **«Внешняя защита»**

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Организации, посетители, сотрудники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов Организации.

Для обеспечения безопасности ПДн необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим Организации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

10 **Безопасность персональных данных**

10.1. Организация при обработке ПДн **обязана** принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

10.2. Использование и хранение биометрических ПДн вне ИСПДн могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают

безопасность этим данным от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

11 Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

11.1 Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему ПДн, несет персональную ответственность за данное разрешение.

11.2 Каждый сотрудник Организации, получающий для работы конфиденциальный документ, указанный в п. 11.1, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

11.3 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.