



ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ КОМИ
«СЫСОЛЬСКАЯ ЦЕНТРАЛЬНАЯ РАЙОННАЯ БОЛЬНИЦА»
с. Визинга

«СЫКТЫВ РАЙОНСА ШОР БОЛЬНИЧА»
КОМИ РЕСПУБЛИКАСА ЙӨЗЛҮСЬ ДЗОНЬВИДЗАЛУН ВИДЗАН КАНМУ СҮЁМКУД УЧРЕЖДЕНИЕ



УТВЕРЖДАЮ

Главный врач ИВУЗ РК «Сысольская ЦРБ»
В.Г. Носков
2014 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных

Оглавление

Термины и определения	3
Сокращения и обозначения.....	5
1. Общие положения.....	6
2. Состав персональных данных.....	7
3. Цели, основания, условия прекращения обработки персональных данных	8
4. Обработка персональных данных	10
4.1. Общие положения.....	10
4.2. Условия обработки	10
4.3. Объем	12
4.4. Согласие субъекта персональных данных	13
4.5. Сбор.....	14
4.6. Хранение.....	15
4.7. Уничтожение.....	16
4.8. Условия обезличивания	17
4.9. Нарушения при обработке	18
4.10. Особенности автоматизированной обработки.....	18
4.11. Особенности неавтоматизированной обработки.....	19
4.12. Поручение обработки.....	20
5. Доступ к персональным данным	22
6. Защита персональных данных	25
7. Ответственность.....	28

Термины и определения

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

База данных – совокупность данных, организованных по определенным правилам, предусматривающих общие принципы описания, хранения и манипулирования данными, независимая от прикладных программ.

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.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных.

Доступ к информации - возможность получения информации и ее использования.

Информационные ресурсы - это организованная совокупность документированной информации, включающая базы данных и знаний, массивы.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

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

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

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичным им по своим функциональному предназначению и техническим характеристикам.

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 характеристиках физических величин.

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

Система защиты персональных данных - система включающая в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

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.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Сокращения и обозначения

АРМ – автоматизированное рабочее место;
ИСПДн – информационная система персональных данных;
МНИ – машинный носитель информации;
НСД – несанкционированный доступ;
ОС – операционная система;
ПДК – постоянно действующая комиссия по защите персональных данных;
ПДн – персональные данные;
ПО – программное обеспечение;
Положение – положение об обработке и защите персональных данных;
СЗПДн – система защиты персональных данных;
УБПДн – угроза безопасности персональных данных;
Учреждение – ГБУЗ РК «Сысольская ЦРБ».

1. Общие положения

- 1.1. Настоящее положение определяет особенности обработки персональных данных в Учреждении, осуществляющей с использованием средств вычислительной техники и без использования таких средств.
- 1.2. Настоящее Положение определяет состав основных правовых, организационных, технических и иных мер по обеспечению режима защиты ПДн в Учреждении.
- 1.3. Целями настоящего Положения являются:
 - 1.3.1. обеспечение защиты прав и свобод субъектов ПДн при обработке их ПДн в ИСПДн Учреждения;
 - 1.3.2. установление ответственности должностных лиц Учреждения, имеющих доступ к ПДн, за невыполнение требований и норм законодательства Российской Федерации и локальных нормативных актов Учреждения, регламентирующих обработку и защиту ПДн.
- 1.4. Действие Положения распространяется на всех работников Учреждения, осуществляющих обработку ПДн, и на всех субъектов ПДн, чьи ПДн обрабатываются в Учреждении.
- 1.5. Работники Учреждения, на которых распространяется действие Положения должны быть ознакомлены с ним под роспись в Журнале учета ознакомлений с локальными нормативными актами.
- 1.6. Методическое руководство работниками Учреждения и контроль над соблюдением требований настоящего Положения возлагается на ПДК.
- 1.7. Настоящий документ вступает в силу со дня его утверждения приказом главного врача.
- 1.8. Изменения, а также признание настоящего Положения утратившим силу осуществляется на основании приказа главного врача Учреждения.

2. Состав персональных данных

2.1. Субъектами ПДн в Учреждении являются:

- работники Учреждения;
- пациенты;
- законные представители пациента.

2.2. Состав обрабатываемых ПДн с указанием субъектов ПДн, целью обработки ПДн, обоснованием необходимости обработки ПДн, сроков хранения ПДн определяется Перечнем обрабатываемых персональных данных.

2.3. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн в Учреждении не обрабатываются.

2.4. Сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни субъектов ПДн в Учреждении не обрабатываются.

3. Цели, основания, условия прекращения обработки персональных данных

3.1. Обработка ПДн работников осуществляется в целях:

- обеспечения соблюдения конституционных прав работников, а также норм и требований законодательства Российской Федерации о государственной социальной помощи, о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях, трудового законодательства;
- исполнения обязательств и функций работодателя;
- ведения кадрового делопроизводства и бухгалтерского учета;
- расчета, начисления и выдачи заработной и иной платы;
- осуществления отчислений в пенсионные фонды, федеральную налоговую службу, фонды социального страхования;
- содействия в осуществлении трудовой (служебной) деятельности и учета результатов исполнения договорных обязательств;
- обучения, повышения квалификации и продвижения по службе;
- предоставления льгот;
- контроля количества и качества выполняемой работы.

3.2. Обработка ПДн работников осуществляется на основании:

- трудового кодекса РФ;
- налогового кодекса РФ;
- устава Учреждения;
- трудового договора с работником.

3.3. Обработка ПДн работников прекращается в случаях:

- достижения целей обработки ПДн;
- расторжения трудового договора или по его окончанию;
- возврата согласия субъекта ПДн на обработку его ПДн.

3.4. Обработка ПДн пациентов осуществляется в целях:

- исполнения федерального закона Российской Федерации от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- исполнения федерального закона Российской Федерации от 19 ноября 2010 г. №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

3.5. Обработка ПДн пациентов осуществляется на основании:

- гражданского кодекса РФ;

- устава Учреждения;
- федерального закона Российской Федерации от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- федерального закона Российской Федерации от 19 ноября 2010 г. №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- согласия субъекта (законного представителя субъекта ПДн).

3.6. Обработка ПДн пациентов прекращается в случаях:

- достижения целей обработки ПДн;
- отзыва субъектом ПДн данного ранее согласия на обработку ПДн.

3.7. Обработка ПДн законных представителей пациентов осуществляется в целях:

- оказания медицинских услуг пациенту;
- исполнения федерального закона Российской Федерации от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

3.8. Обработка ПДн законных представителей пациентов осуществляется на основании:

- устава Учреждения;
- федерального закона Российской Федерации от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- согласия субъекта ПДн.

3.9. Обработка ПДн законных представителей прекращается в случаях:

- достижения целей обработки ПДн;
- отзыва субъектом ПДн данного ранее согласия на обработку ПДн.

4. Обработка персональных данных

4.1. Общие положения

- 4.1.1. Обработка ПДн в Учреждении осуществляется на законной и справедливой основе.
- 4.1.2. Субъект ПДн является собственником своих ПДн и самостоятельно принимает решение о передаче их Учреждению.
- 4.1.3. Держателем ПДн субъектов ПДн является Учреждение, которому субъекты ПДн добровольно передают во владение свои ПДн. Учреждение выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством РФ.
- 4.1.4. Потребителями ПДн являются юридические и физические лица, обращающиеся к собственнику и (или) держателю ПДн за получением необходимых сведений и пользующиеся ими без права предоставления и распространения.
- 4.1.5. При обработке ПДн, работниками Учреждения обеспечивается их точность, достаточность и актуальность по отношению к целям их сбора.
- 4.1.6. При обработке ПДн, главный врач определяет способы обработки, документирования, хранения и защиты ПДн на базе современных информационных технологий.

4.2. Условия обработки

- 4.2.1. ПДн субъектов ПДн обрабатываются в Учреждении как с использованием средств вычислительной техники, так и без использования таких средств.
- 4.2.2. Обработка ПДн ограничивается достижением определенных настоящим положением целей.
- 4.2.3. Не допускается обработка ПДн, несовместимая с целями их сбора.
- 4.2.4. Не допускается использование ПДн в целях причинения имущественного и морального вреда субъектам ПДн, а также затруднения реализации их прав и свобод. Ограничение прав граждан РФ на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством РФ.
- 4.2.5. Обработка ПДн допускается в следующих случаях:
 - обработка ПДн осуществляется с согласия субъекта ПДн;
 - обработка ПДн необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и

выполнения, возложенных законодательством РФ на Учреждение функций, полномочий и обязанностей;

- 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;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- обработка ПДн необходима для осуществления прав и законных интересов Учреждения или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- обработка ПДн осуществляется в статистических или иных исследовательских целях, за исключением целей, связанных с политической агитацией, продвижением товаров, работ и услуг на рынке;
- осуществляется обработка ПДн, доступ неограниченного круга лиц к которому предоставлен субъектом ПДн либо по его просьбе;
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством РФ.

4.2.6. Учреждение не имеет право получать и обрабатывать специальные категории ПДн субъектов ПДн, за исключением случаев, если:

- субъект ПДн дал согласие в письменной форме на обработку своих ПДн;
- ПДн сделаны общедоступными субъектом ПДн;
- обработка ПДн осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством РФ о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;
- обработка ПДн осуществляется в медик-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 РФ сохранять врачебную тайну;

- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;
- обработка ПДн осуществляется в соответствии с законодательством РФ об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством РФ;
- обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

4.2.7. Должностное лицо Учреждения, ответственное за кадровое обеспечение, обязано проводить дополнительные мероприятия, направленные на подтверждение факта направления резюме самим соискателем, в случае получения указанного резюме по каналам электронной почты или факсимильной связи.

4.2.8. Резюме, составленные в произвольной форме, при которой не представляется возможным однозначно определить физическое лицо его направившее, подлежат уничтожению в течение десяти рабочих дней с момента их поступления.

4.2.9. Ответственные работники Учреждения разъясняют субъектам ПДн юридические последствия их отказа в предоставлении своих ПДн, если предоставление ПДн является обязательным в соответствии с законодательством РФ (трудовым законодательством, законодательством о медицинском, пенсионном и социальном страховании и др.).

4.2.10. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.2.11. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на ПДн работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель должен учитывать личные качества работника, его добросовестный и эффективный труд.

4.3. Объем

4.3.1. Объем и состав обрабатываемых в Учреждении ПДн соответствует заявленным целям сбора. Не допускается обработка ПДн являющихся избыточными по отношению к заявленным целям сбора.

4.4. Согласие субъекта персональных данных

4.4.1. Обработка ПДн работника не требует получения его согласия, при условии, что объем обрабатываемых Учреждением ПДн не превышает установленные перечни, а также соответствует целям обработки, предусмотренным трудовым законодательством.

4.4.2. Обработка ПДн уволенного работника Учреждения не требует получения соответствующего согласия, при условии, что обработка ПДн осуществляется в рамках бухгалтерского и (или) налогового учета и соблюдаются сроки, предусмотренные законодательством РФ. После истечения сроков, предусмотренных законодательством РФ, личные дела работников и иные документы передаются на архивное хранение, при этом, на организацию архивного хранения, комплектование, учет и использование архивных документов, содержащих ПДн работников, действие Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» не распространяется.

4.4.3. Письменное согласие субъекта ПДн на обработку его ПДн включает 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 и адрес местонахождения Учреждения;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта ПДн;
- пункт о согласии субъекта ПДн на включение его ПДн в общедоступные источники ПДн (в том числе справочники, адресные книги и т.п.), с указанием состава включаемых ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Учреждения, если обработка будет поручена такому лицу;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Учреждением способов обработки ПДн;
- срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта ПДн.

4.4.4. Получение согласий субъектов ПДн на обработку их ПДн в письменной форме требуется в случаях, если:

- Учреждение осуществляет передачу ПДн субъектов ПДн третьим лицам, не установленную законодательством РФ;
- Учреждение формирует (организует) общедоступные источники ПДн (в том числе справочники, адресные книги), не установленные законодательством РФ;
- Учреждение намеревается получать ПДн субъектов ПДн от третьих лиц, в том числе направлять запросы по прежним местам работы для уточнения или получения дополнительной информации;
- Учреждение осуществляет обработку специальных категорий ПДн субъектов ПДн, за исключением случаев, когда обработка специальных категорий ПДн допускается без согласия субъекта ПДн в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

4.4.5. Учреждение вправе без соответствующего согласия осуществлять обработку ПДн работника, в случаях, предусмотренных коллективным договором, в том числе правилами внутреннего трудового распорядка, являющимися приложением к коллективному договору, соглашением, а также локальными нормативными актами Учреждения, принятymi в порядке, установленном ст. 372 Трудового кодекса РФ.

4.4.6. В случаях, предусмотренных законодательством РФ, согласие на обработку ПДн субъекта ПДн дает его законный представитель.

4.4.7. Субъект ПДн имеет право в любое время отозвать данное ранее согласие на обработку своих ПДн.

4.4.8. Субъект ПДн имеет право в любое время потребовать от Учреждения исключить сведения о себе из созданных ранее общедоступных источников ПДн (в том числе справочников, адресных книг). Сведения о субъекте ПДн также исключаются из общедоступных источников ПДн по решению суда или иных уполномоченных государственных органов.

4.5. Сбор

4.5.1. Все ПДн субъектов ПДн Учреждение получает от них самих или их законных представителей.

4.5.2. В случае невозможности получения ПДн субъекта ПДн от него самого, Учреждение имеет право получить ПДн этого субъекта ПДн от третьей

стороны, при условии наличия оснований, указанных в п.4.2.4 настоящего положения и предварительного уведомления субъекта ПДн о получении его ПДн от третьей стороны. В уведомлении указываются цели, предполагаемые источники и способы получения ПДн.

4.5.3. Учреждение освобождается от обязанности уведомления субъекта ПДн о получении его ПДн от третьей стороны в случаях, если:

- Субъект ПДн уведомлен об осуществлении обработки его ПДн Учреждением;
- ПДн получены Учреждением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- Учреждение осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта ПДн;
- Уведомление субъекта ПДн нарушает права и законные интересы третьих лиц.

4.6. Хранение

4.6.1. Сроки хранения документов, содержащих ПДн субъектов ПДн, а также сроки хранения сведений, содержащих ПДн субъектов ПДн в электронном виде (электронные документы, записи баз данных) определяются Перечнем обрабатываемых ПДн в соответствии с приказом Министерства культуры РФ от 25 августа 2010 г. № 558 «Об утверждении «Перечня типовых управленических архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», номенклатурой дел, сроком исковой давности, а также иными требованиями законодательства РФ».

4.6.2. Все меры конфиденциальности при обработке ПДн субъектов ПДн распространяются как на бумажные, так и на МНИ.

4.6.3. Места хранения ПДн, а также документов и МНИ их содержащих, определяются Перечнем хранилищ ПДн и их материальных носителей.

4.6.4. ПДн в электронном виде содержатся в виде электронных документов, таблиц и записей баз данных на АРМ работников.

- 4.6.5. Документы, законченные делопроизводством, хранятся централизованно в архиве Учреждения или в структурных подразделениях в соответствии с установленными им сроками хранения.
- 4.6.6. Хранение ПДн осуществляется в порядке, исключающем их утрату, неправомерное использование или НСД к ним.
- 4.6.7. Материальные носители ПДн (бумажные, машинные) хранятся в кабинетах ответственных работников Учреждения в запираемых шкафах, ящиках столов или сейфах.
- 4.6.8. 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. Обрабатываемые ПДн подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.7. Уничтожение

- 4.7.1. В случае достижения целей обработки ПДн, обработка ПДн прекращается и ПДн (или их материальные носители) подлежат уничтожению в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Учреждением и субъектом ПДн, либо если Учреждение не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ.
- 4.7.2. Уничтожение носителей ПДн производится после поступления от руководителей структурных подразделений, обрабатывающих ПДн, в ПДК перечня (в том числе в электронном виде) подлежащих уничтожению носителей ПДн с указанием основания для их уничтожения.
- 4.7.3. Уничтожение ПДн на МНИ производится после истечения сроков хранения ПДн ПДК с использованием специального программного обеспечения или средств гарантированного уничтожения информации. Об уничтожении (стирании) ПДн на МНИ ПДК составляется акт.
- 4.7.4. Способ уничтожения носителей ПДн должен исключать возможность восстановления уничтоженных ПДн.

4.7.5. Бумажные носители ПДн уничтожаются исполнителем в присутствии членов ПДК с оформлением акта по следующей процедуре:

- включение каждого отобранного к уничтожению документа (дела) отдельной позицией в акт;
- оформление в акте итоговой записи с указанием количества уничтожаемых документов (дел), подписание итоговой записи членами ПДК, составившими акт;
- подписание акта членами ПДК;
- утверждение акта главным врачом Учреждения.

4.7.6. Перед непосредственным уничтожением носителей ПДн членами ПДК осуществляется сверка документов и дел с описью, приведенной в акте уничтожения.

4.7.7. Бумажные носители ПДн уничтожаются в присутствии членов ПДК в составе не менее 3 человек, принимавших участие в сверке (проверке) документов (дел), подлежащих уничтожению. После уничтожения документов (дел) члены ПДК производят запись в акте об уничтожении, заверяют ее своими подписями.

4.7.8. Уничтожение документов производится путем сожжения, дробления, растворения или химического разложения, превращения в бесформенную массу или порошок. Допускается уничтожение документов путем измельчения в кусочки площадью не более 2,5 кв. мм.

4.8. Условия обезличивания

4.8.1. Обезличивание ПДн может быть проведено с целью ведения статистических наблюдений, снижения потенциального ущерба от разглашения ПДн и по достижению целей обработки ПДн или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством РФ.

4.8.2. Способы обезличивания ПДн при условии дальнейшей их обработки:

- сокращение состава обрабатываемых ПДн;
- обобщение/понижение точности некоторых ПДн;
- разделение ПДн на части, и обработка в разных ИСПДн.

4.8.3. Решение о необходимости обезличивания ПДн принимает главный врач Учреждения.

4.8.4. ПДК непосредственно с ответственными за обработку ПДн работниками готовят предложения главному врачу Учреждения по обезличиванию ПДн с обоснованием такой необходимости и способа обезличивания.

4.8.5. Лица, ответственные за проведение мероприятий по обезличиванию обрабатываемых ПДн назначаются приказом главного врача Учреждения.

4.9. Нарушения при обработке

4.9.1. В случае выявления неправомерной обработки ПДн, ПДК осуществляет блокирование неправомерно обрабатываемых ПДн, на период проверки, и в срок, не превышающих пяти рабочих дней с даты этого выявления, прекращает неправомерную обработку ПДн.

4.9.2. В случае если обеспечить правомерность обработки ПДн невозможно, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, уничтожает такие ПДн.

4.9.3. Об устраниении допущенных нарушений или об уничтожении ПДн Учреждение уведомляет субъекта ПДн.

4.9.4. В случае выявления неточных ПДн, Учреждение осуществляет блокирование ПДн, относящихся к этому субъекту ПДн на период проверки или уточнения ПДн, если это не нарушает права и законные интересы субъекта ПДн.

4.10. Особенности автоматизированной обработки

4.10.1. Обработка ПДн с использованием средств вычислительной техники осуществляется в ИСПДн Учреждения. Определение необходимости обеспечения установленных Правительством РФ уровней защищенности ПДн при их обработке в ИСПДн Учреждения осуществляется ПДК, в порядке, установленном Правительством РФ.

4.10.2. Безопасность ПДн обрабатываемых в ИСПДн Учреждения обеспечивается путем исключения НСД, в том числе случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий в отношении ПДн.

4.10.3. ПДК при обработке ПДн в ИСПДн Учреждения обеспечивается их безопасность с помощью СЗПДн, включающей организационные и технические средства защиты информации, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.

4.10.4. Доступ к АРМ и ресурсам ИСПДн осуществляется в соответствии с Положением о разграничении прав доступа к ресурсам ИСПДн, на основании Перечней прав доступа к ресурсам ИСПДн.

4.10.5. Доступ к ресурсам ИСПДн предоставляется после прохождения процедур идентификации и аутентификации.

4.10.6. МНИ, предназначенные для хранения и обработки ПДн, подлежат обязательной регистрации и учету в Журнале учета материальных носителей информации.

4.10.7. Требования к учету, хранению и уничтожению МНИ определяются Регламентом учета хранения и уничтожения МНИ.

4.10.8. Требования к работникам, осуществляющим автоматизированную обработку ПДн, определяются Инструкциями и другими локальными нормативными актами Учреждения.

4.10.9. Работники Учреждения допускаются к работе с ИСПДн только после ознакомления с локальными нормативными актами Учреждения, регламентирующими обработку и защиту ПДн.

4.11. Особенности неавтоматизированной обработки

4.11.1. ПДн при их обработке, осуществляющейся без использования средств вычислительной техники, обособляются от иной информации, в частности, путем фиксации их на отдельных носителях, в специальных разделах или на полях форм (бланков).

4.11.2. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо несовместимы. Для обработки ПДн разных категорий субъектов ПДн используются отдельные бумажные носители.

4.11.3. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, применяются следующие меры по обеспечению раздельной обработки ПДн:

- при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется копия ПДн;
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению

или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

- 4.11.4. Уничтожение или обезличивание ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.
- 4.11.5. Документы на бумажных носителях, содержащие ПДн, хранятся раздельно в зависимости от целей их обработки.
- 4.11.6. Уточнение ПДн при осуществлении их обработки без использования средств вычислительной техники производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.
- 4.11.7. Работники Учреждения, хранящие ПДн на бумажных носителях, обеспечивают их защиту от НСД согласно «Положению об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации», утвержденному постановлением правительства РФ от 15.09.2008 г. № 687.

4.12. Поручение обработки

- 4.12.1. Учреждение вправе поручать обработку ПДн другому лицу с согласия субъекта ПДн, на основании заключаемого с этим лицом договора.
- 4.12.2. Уполномоченное на обработку ПДн лицо обязано соблюдать принципа и правила обработки ПДн, предусмотренные Федеральным законом от 27.08.2006 г. № 152-ФЗ «О персональных данных».
- 4.12.3. В поручении на обработку ПДн определяется перечень действий (операций) с ПДн, которые будут совершаться уполномоченным на обработку лицом и цели обработки ПДн, а также указываются требования к их защите в соответствии с законодательством Российской Федерации.
- 4.12.4. Уполномоченное лицо не обязано получать согласие субъектов ПДн на обработку их ПДн.
- 4.12.5. В случае если Учреждение поручает обработку ПДн уполномоченному на обработку ПДн лицу, ответственность перед субъектом ПДн за действия указанного лица несет Учреждение. Уполномоченное на обработку ПДн лицо несет ответственность перед Учреждением.

5. Доступ к персональным данным

- 5.1. Работники Учреждения получают доступ к ПДн субъектов ПДн в объеме, необходимом для выполнения своих должностных обязанностей, после ознакомления с локальными нормативными актами Учреждения, устанавливающими порядок обработки и защиты ПДн.
- 5.2. Порядок оформления доступа к ПДн, его изменение или прекращение регламентируется отдельным Положением о разграничении доступа к обрабатываемым ПДн в Учреждении.
- 5.3. Список работников Учреждения, имеющих доступ к ПДн субъектов ПДн на бумажных носителях, определяется Перечнем работников, допущенных к неавтоматизированной обработке ПДн.
- 5.4. Списки лиц, имеющих доступ к ресурсам ИСПДн Учреждения определяются Перечнями прав доступа к ресурсам ИСПДн.
- 5.5. Работник Учреждения получает доступ к ПДн субъектов после:
- подписания обязательства о неразглашении ПДн;
 - ознакомления и изучения требований настоящего положения и иных локальных нормативных актов Учреждения, регламентирующих обработку ПДн в части, его касающейся;
 - прохождения инструктажа о соблюдении правил обработки и защиты ПДн в Учреждении;
 - ознакомления с видами ответственности за нарушение (невыполнение) норм законодательства РФ в сфере обработки и защиты ПДн.
- 5.6. Субъект ПДн имеет право на получение сведений о наличии у Учреждения его ПДн, а также на ознакомление с ними, в том числе на безвозмездное получение копии любой записи, содержащей его ПДн за исключением случаев, предусмотренных законодательством РФ.
- 5.7. Субъект ПДн имеет право запрашивать у Учреждения следующие сведения:
- подтверждение факта обработки ПДн Учреждением;
 - основания и цели обработки ПДн;
 - способы обработки ПДн;
 - сведения о лицах, которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Учреждением или на основании федерального закона;
 - сроки обработки ПДн, в том числе сроки их хранения;
 - иные сведения, предусмотренные законодательством РФ.

- 5.8. Право субъекта ПДн на доступ к его ПДн ограничивается, в случае нарушения при таком доступе прав и свобод других субъектов ПДн.
- 5.9. Письменный запрос субъекта ПДн должен быть удостоверен следующими документами:
- паспортом или другим документов удостоверяющим личность субъекта ПДн (в случае непосредственного обращения субъекта ПДн с запросом в Учреждение);
 - нотариально заверенной подписью (в случае направления в Учреждение почтового запроса);
 - документом, подтверждающим полномочия законного представителя субъекта ПДн (в случае направление в Учреждения запроса от законного представителя ПДн, при этом непосредственно запрос должен быть удостоверен одним из вышеперечисленных способов).
- 5.10. Принципы реагирования на обращения (запросы) субъектов ПДн (их представителей) определяются Регламентом реагирования на обращения субъектов ПДн.
- 5.11. Все поступившие письменные запросы субъектов ПДн (и их законных представителей) регистрируются ответственным за реагирование на обращения субъектов ПДн в Журнале учета обращений субъектов ПДн, а затем направляются ответственному работнику для подготовки ответа субъекту ПДн не позднее пяти рабочих дней с момента поступления обращения в Учреждения.
- 5.12. Ответ в письменной форме на обращение субъекта ПДн формируется ответственным работником, подписывается главным врачом Учреждения в течение десяти рабочих дней с даты поступления в Учреждение запроса от субъекта ПДн и отправляется ответственным за реагирование на обращения субъектов ПДн в срок, не превышающий трех рабочих дней, в адрес субъекта ПДн через отделение почтовой связи заказным письмом с уведомлением о вручении или курьером (непосредственно в руки адресату под подпись).
- 5.13. Субъект ПДн вправе требовать от Учреждения 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, а также принимать предусмотренные законом меры по защите своих прав.
- 5.14. Доступ третьих лиц к ПДн субъектов ПДн осуществляется только с их письменного согласия, за исключением случаев, когда такой доступ необходим в

целях предупреждения угрозы жизни и здоровью субъекта ПДн или других лиц и иных случаев, установленных законодательством РФ, в минимальных объемах и только в целях выполнения задач, соответствующих объективной цели сбора этих данных.

5.15. Предоставление ПДн работников Учреждения третьим, в том числе должностным, лицам без их согласия допускается:

- в рамках обязательного социального страхования работников Учреждения, в порядке, установленном федеральными законами;
- в случаях предоставления ПДн работников Учреждения в налоговые органы, военные комиссариаты и профсоюзные органы в соответствии с законодательством РФ;
- в рамках открытия и (или) обслуживания платежных карт для начисления заработной платы, при условии соблюдения одного из следующих положений:
 - договор на выпуск банковской карты заключался напрямую с работником Учреждения и в тексте которого предусмотрены положения, предусматривающие передачу Учреждением ПДн работника;
 - Учреждение имеет доверенность на представление интересов работника при заключении договора с кредитной организацией на выпуск банковской карты и ее последующем обслуживании;
 - Соответствующая форма и система оплаты труда прописана в договоре.

6. Защита персональных данных

- 6.1. Учреждение самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения безопасности ПДн, в соответствии с требованиями законодательства РФ в области защиты ПДн.
- 6.2. Кроме мер защиты ПДн, установленных законодательством РФ, Учреждение вправе разрабатывать и внедрять собственные меры защиты ПДн, не противоречащие требованиям законодательства РФ.
- 6.3. В Учреждении принимаются необходимые правовые, организационные и технические меры, обеспечивающие защиту ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий в отношении ПДн в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в ИСПДн, утвержденными постановлением Правительства от 01.11.2012 г. № 1119.
- 6.4. Защита ПДн субъектов ПДн от неправомерного их использования или утраты обеспечивается за счет средств Учреждения, в порядке, установленном законодательством РФ.
- 6.5. Защита ПДн представляет собой динамический технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности ПДн и, в конечном счете, обеспечивающий необходимый уровень защищенности, установленный Правительством РФ.
- 6.6. Порядок проведения конкретных мероприятий по защите ПДн с использованием или без использования средств вычислительной техники определяется приказами главного врача Учреждения и иными локальными нормативными актами.
- 6.7. В целях исполнения настоящего положения и на основании Положения о постоянно действующей комиссии по защите ПДн и Регламента проведения внутренних мероприятий по контролю обеспечения защиты ПДн, ПДК ежегодно составляет и утверждает у главного врача Учреждения Годовой план мероприятий по поддержанию режима защиты ПДн ПДК.
- 6.8. Проводимые в Учреждении мероприятия по обеспечению безопасности ПДн регистрируются ответственным лицом в Журнале по учету мероприятий по контролю обеспечения защиты ПДн.
- 6.9. В целях организации и проведения работ по обеспечению безопасности ПДн в Учреждении, приказом главного врача Учреждения назначаются:

6.9.1. ПДК, ответственная за проведение мероприятий по обеспечению безопасности ПДн, поддержание необходимого уровня информационной безопасности и проведение инструктажа работников по основам информационной безопасности при работе с ПДн;

6.9.2. Администратор ИСПДн, ответственный за установку, настройку, администрирование и обслуживание ПО и средств защиты информации, применяемых в Учреждении для обработки ПДн.

6.10. ПДК ответственна за проведение следующих мероприятий по обеспечению безопасности ПДн:

- определение и описание ИСПДн;
- определения уровней защищенности ПДн при их обработке в ИСПДн;
- определение актуальных УБПДн;
- проектирование СЗПДн, включающей организационные, физические и технические меры и средства защиты;
- закупку, установку и настройку технических средств защиты информации;
- внедрение, организацию, разработку мероприятий и необходимых положений, регламентов и инструкций;
- инструктаж и обучение работников, участвующих в обработке ПДн.

6.11. ПДК для внедрения, настройки и администрирования ТСЗИ может привлекать стороннюю организацию, имеющую лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

6.12. Председатель ПДК назначает лиц, из членов ПДК, ответственных за соблюдение требований настоящего положения и других локальных нормативных актов Учреждения, регламентирующих обработку и защиту ПДн.

6.13. Контроль выполнения работ по обеспечению безопасности ПДн в Учреждении осуществляется путем проведения периодических контрольных мероприятий и внутренних проверок согласно Регламенту проведения внутренних мероприятий по контролю обеспечения защиты персональных данных.

6.14. Ежегодно ПДК направляет главному врачу Учреждения отчет о проведенных мероприятиях по выполнению Годового плана мероприятий по поддержанию режима защиты ПДн, вместе с перечнем предложений по совершенствованию СЗПДн.

6.15. Необходимость проведения мероприятий по совершенствованию СЗПДн может быть обусловлена:

- результатами проведенных аудитов и контрольных мероприятий;

- изменениями федерального законодательства в области ПДн;
- изменениями структуры процессов обработки ПДн в Учреждении;
- результатами мероприятий по контролю и надзору за обработкой ПДн, проводимых уполномоченным органом;
- жалобами и запросами субъектов ПДн.

6.16. На основании решения, принятого главным врачом Учреждения по результатам рассмотрения ежегодного отчета и предложений по совершенствованию СЗПДн, ПДК составляет Годовой план мероприятий по поддержанию режима защиты ПДн ПДК на следующий год.

7. Ответственность

- 7.1. Председатель ПДК несет персональную ответственность за организацию и поддержание режима защиты ПДн в Учреждении.
- 7.2. Члены ПДК несут персональную ответственность за своевременное и качественное исполнение возложенных на них задач и функций в соответствии с локальными нормативными актами, регламентирующими обработку и защиту ПДн.
- 7.3. Работники, виновные в нарушении норм обработки и защиты ПДн, определенных законодательством РФ и локальными нормативными актами несут дисциплинарную, гражданскую, административную, уголовную и иную ответственность, предусмотренную законодательством РФ.
- 7.4. Разглашение охраняемой законом тайны (государственной, коммерческой, врачебной, служебной и иной), ставшей известной работнику в связи с исполнением трудовых обязанностей, в том числе разглашение ПДн субъектов ПДн, влечет расторжение трудового договора с работником по инициативе работодателя (ст.81 ТК РФ) и наложение административного штрафа на должностное лицо в размере, предусмотренном кодексом РФ об административных правонарушениях (ст.13.14 КоАП РФ).
- 7.5. Неисполнение или ненадлежащее исполнение работником возложенных на него обязанностей и функций по соблюдению установленного порядка обработки и защиты ПДн влечет замечание, выговор или увольнение работника по соответствующим основаниям (ст.192 ТК РФ).
- 7.6. Нарушение установленного законом порядка сбора, хранения, использования и распространения ПДн влечет предупреждение или наложение административного штрафа на должностное лицо в размере, предусмотренном кодексом РФ об административных правонарушениях (ст.13.11 КоАП РФ).
- 7.7. Незаконный сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующимся произведении или средствах массовой информации влечет наказание в соответствии с Уголовным кодексом РФ (ст.137 УК РФ).
- 7.8. Неправомерный отказ в предоставлении собранных в установленном порядке ПДн, либо предоставление неполных или заведомо ложных сведений, если эти деяния причинили вред правам и законным интересам субъекта ПДн влечет

наказание в соответствии с Уголовным кодексом РФ (ст.5.39 КоАП РФ, ст.140 УК РФ).

7.9. Неправомерный доступ к охраняемой законом компьютерной информации, т. е. информации на машинном носителе, в ЭВМ, системе ЭВМ или сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети влечет наказание в соответствии с Уголовным кодексом РФ (ст.272 УК РФ).

