УТВЕРЖДАЮ
Главный врач МБУЗ АР
«Стоматологическая поликлиника»
_____ Г.А. Айрапетов
«17» января 2022

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ ЗДРАВООХРАНЕНИЯ АКСАЙСКОГО РАЙОНА «СТОМАТОЛОГИЧЕСКАЯ ПОЛИКЛИНИКА»

Аксай 2022

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика информационной безопасности (далее – Политика) разработана в соответствии с Конституцией Российской Федерации, Федеральным законом Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных», а также иными нормативно-правовыми актами, регламентирующими порядок обращения с персональными данными (далее - законодательство) и устанавливает единый порядок работы с персональными данными (далее - ПДн) пациентов и иных физических лиц (далее - субъектов), обрабатываемыми в муниципальном бюджетном учреждении здравоохранения Аксайского района «Стоматологическая поликлиника» (далее - учреждение).

1.2. Политика разработана в следующих целях:

- защита ПДн субъектов, обрабатываемых в Учреждении, от несанкционированного доступа и разглашения;
- обеспечение защиты прав и свобод субъектов при обработке их ПДн в Учреждении;
- предотвращение нарушений законных прав и интересов субъектов при обработке их ПДн в Учреждении;
- установление мер ответственности должностных лиц, имеющих доступ и доступ к ПДн субъектов в Учреждении, за невыполнение/нарушение требований законодательства, регулирующего обработку ПДн;
- недопущения нанесения возможного ущерба, вызванного неправомерными умышленными или неосторожными действиями юридических и (или) физических лиц путем безвозмездного присвоения информации или ее разглашения, нарушения норм, регулирующих обработку и защиту ПДн субъектов;

1.3. Все сотрудники Учреждения, допущенные к обработке ПДн субъектов, должны быть ознакомлены с данной Политикой.

1.4. Учреждение, как оператор, назначает лицо, ответственное за организацию обработки ПДн в Учреждении.

Основные понятия, используемые в настоящей Политике

Персональные данные субъектов - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

Обработка персональных данных - 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;

Автоматизированная обработка персональных данных - обработка ПДн с помощью средств вычислительной техники;

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

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

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

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители, содержащие ПДн;

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

Информационная система персональных данных (ИСПДн) – совокупность содержа-

щихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

Трансграничная передача персональных данных - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

Информация - сведения (сообщения, данные) независимо от формы их представления.

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2. ПОНЯТИЕ И СОСТАВ ПДн СУБЪЕКТА

Состав обрабатываемых ПДн субъектов зависит от целей обработки ПДн, осуществляемых в соответствии с Уставом Учреждения.

2.1. Информация, содержащая ПДн субъектов, используется в Учреждении в целях:

- оказания медицинских услуг, ведения персонифицированного учета в сфере обязательного медицинского страхования в соответствии с действующим законодательством;
- оформления документации, установленной действующим законодательством;
- выполнения функций, обязанностей и задач, возложенных на Учреждение законодательством;
- оформления и выполнения договорных, преддоговорных отношений по направлениям своей деятельности.

2.2. Состав обрабатываемых ПДн субъектов может меняться, исходя из требований законодательства.

3. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ

Права субъектов ПДн

Субъект ПДн обладает правами, определенными законодательством.

3.1. Субъект ПДн имеет право:

3.1.1. 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 меры, предусмотренные законом по защите своих прав;

3.1.2. Требовать от Учреждения при обращении или направлении запроса[1] предоставления сведений о наличии его ПДн в доступной форме. При этом в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

Запрос должен отвечать требованиям законодательства о ПДн. При этом подлежит предоставлению следующая информация:

1) подтверждение факта обработки ПДн субъекта Учреждением;
2) правовые основания и цели обработки ПДн;
3) цели и способы обработки ПДн, применяемые в Учреждении;
4) наименование и место нахождения Учреждения, сведения о лицах (за исключением сотрудников Учреждения), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Учреждением или на основании федерального закона;
5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
6) сроки обработки ПДн, в том числе сроки их хранения;
7) порядок осуществления субъектом ПДн прав, предусмотренных законодательством;
8) информацию об осуществляемой или о предполагаемой трансграничной передаче данных;
9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку

---

[1] С данным запросом вправе обратиться представитель субъекта ПДн.

ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные законодательством.

Право на доступ субъекта ПДн к его ПДн ограничивается в случаях, предусмотренных законодательством;

3.1.3. На защиту своих прав и законных интересов, в том числе на возмещение убытков и(или) компенсацию морального вреда в судебном порядке;

3.1.4. На обжалование действий или бездействие Учреждения в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

3.2. После предоставления необходимых сведений субъекту ПДн по его запросу, последний вправе обратиться повторно в Учреждение или направить ему повторный запрос о предоставлении данных, не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен законодательством, нормативно-правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

3.3. Субъект ПДн вправе обратиться повторно в Учреждение или направить ему повторный запрос в целях получения необходимых сведений, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в п. 3.2. настоящей Политики, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

Повторный запрос наряду со сведениями, предусмотренными законодательством, должен содержать обоснование его направления.

3.4. Учреждение вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным законодательством. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса возлагается на Учреждение.

4. КОНФИДЕНЦИАЛЬНОСТЬ И ЗАЩИТА ПДн СУБЪЕКТОВ

4.1. К информации, содержащей ПДн субъектов, применяется режим конфиденциальности, то есть обязательное для соблюдения получившим доступ к ПДн субъектов лицом требование не раскрывать третьим лицам и не допускать их распространения без согласия субъекта ПДн или иного законного основания.

4.2. Режим конфиденциальности предусматривает:

- Определение перечня должностных лиц, допущенных к обработке ПДн, ответственных за работу с ПДн и сохранность носителей, содержащих ПДн субъектов;
- распределение обязанностей между сотрудниками Учреждения по защите ПДн субъектов;
- ограничение доступа к ПДн субъектов путем установления порядка обращения с этой информацией и контроля за его соблюдением;
- регулирование отношений по использованию ПДн субъектов в рамках договорных отношений;
- принятие мер по выявлению возможных каналов несанкционированного доступа к ПДн субъектов, обеспечение безопасности информации при обработке ПДн субъектов с использованием средств вычислительной техники;
- исключение бесконтрольного использования носителей ПДн субъектов посторонними лицами;
- выделение помещений, предназначенных для работы с ПДн субъектов, с учетом ограничения бесконтрольного доступа сторонних лиц в эти помещения;
- использование необходимых средств защиты ИСПДн;
- организация наллежащего порядка уничтожения информации, содержащей ПДн;
- своевременное выявление нарушений требований разрешительной системы доступа работниками к определенным сведениям;
- информационная работа с сотрудниками по предупреждению нарушения норм законодательства, регулирующего обработку ПДн;
- технические средства охраны, сигнализации;
- принятие иных мер, не противоречащих законодательству.

4.3. Вопросы обеспечения выполнения требований законодательства, методических доку-

ментов, локальных нормативных актов, определяющих порядок защиты ПДн субъектов, возложены на руководителя Учреждения, который координирует и контролирует деятельность всех подразделений при обеспечении конфиденциальности ПДн субъектов.

4.4. Защита ПДн представляет собой комплекс мероприятий, направленных на выявление и предупреждение нарушений доступности, целостности, достоверности и конфиденциальности ПДн в рамках обеспечения безопасности информации в процессе деятельности Учреждения.

4.5. Основным виновником несанкционированного доступа к ПДн является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа работников к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами Учреждения.

5. СБОР, СИСТЕМАТИЗАЦИЯ, ПЕРЕДАЧА, ХРАНЕНИЕ ПДн СУБЪЕКТОВ. ОБЯЗАННОСТИ УЧРЕЖДЕНИЯ

Условия обработки ПДн субъектов

5.1. Обработка ПДн должна осуществляться с соблюдением принципов и правил, предусмотренных законодательством Российской Федерации. Работники Учреждения имеют право обрабатывать только те ПДн субъектов, доступ к которым им необходим в соответствии с их должностными обязанностями.

Обработка ПДн допускается в следующих случаях:

1) обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

2) обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на Учреждении как оператора функций, полномочий и обязанностей;

3) обработка ПДн необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом Российской Федерации от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта ПДн на едином портале государственных и муниципальных услуг;

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;

5) обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

6) обработка ПДн необходима для осуществления прав и законных интересов Учреждения как оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

7) осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн либо по его просьбе (ПДн, сделанные общедоступными субъектом ПДн);

8) обработка ПДн осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания ПДн;

9) осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством.

5.2. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Учреждением.

5.3. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн Учреждение вправе продолжить обработку ПДн без

согласия субъекта ПДн при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».

5.4. Обязанность представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных», возлагается на Учреждение.

5.5. В случаях, предусмотренных федеральным законом, обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта ПДн;

4) цель обработки ПДн;

5) перечень ПДн, на обработку которых дается согласие субъекта ПДн;

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

7) перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

8) срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта ПДн.

5.6. В случае недееспособности субъекта ПДн согласие на обработку его ПДн дает законный представитель субъекта.

5.7. В случае смерти субъекта ПДн согласие на обработку его ПДн дают наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни.

5.8. ПДн могут быть получены Учреждением от лица, не являющегося субъектом ПДн, при условии предоставления Учреждению подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».

Сбор и систематизация ПДн субъектов

5.9. При сборе ПДн Учреждение обязано предоставить субъекту ПДн по его просьбе информацию, предусмотренную п.7 ст.14 Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».

5.10. Законодательством предусматриваются случаи обязательного предоставления субъектом своих ПДн. При отказе субъекта предоставить ПДн Учреждение в обязательном порядке разъясняет юридические последствия такого отказа.

5.11. Организацию и контроль за защитой ПДн субъектов в структурных подразделениях Учреждения, сотрудники которого имеют доступ к ПДн, осуществляют их непосредственные руководители.

5.12. В случае получения ПДн не от субъекта ПДн, Учреждение, до начала обработки таких ПДн, обязано предоставить субъекту информацию, предусмотренную п.3 ст. 18 Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».

Учреждение освобождается от данной обязанности в случаях, предусмотренных законодательством.

5.13. В целях устранения нарушений законодательства, допущенных при обработке ПДн, а также уточнения, блокирования и уничтожения ПДн, Учреждение **обязано:**

5.13.1. При выявлении неправомерной обработки ПДн при обращении субъекта или его представителя либо по запросу субъекта или его представителя либо уполномоченного органа по защите прав субъектов ПДн Учреждение обязано осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неточных ПДн при обращении субъекта или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн Учреждение обязано осуществить блокирование ПДн, относящихся к этому субъекту, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта или третьих лиц.

5.13.2. В случае подтверждения факта неточности ПДн Учреждение на основании сведений, представленных субъектом или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязано уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в течение 7 (семи) рабочих дней со дня представления таких сведений и снять блокирование ПДн.

5.13.3. В случае выявления неправомерной обработки ПДн, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Учреждения. В случае, если обеспечить правомерность обработки ПДн невозможно, Учреждение в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки ПДн, обязано уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Учреждение обязано уведомить субъекта или его представителя, а в случае, если обращение субъекта или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

5.13.4. При достижении цели обработки ПДн Учреждение обязано незамедлительно прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и уничтожить соответствующие ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект, иным соглашением между субъектом и Учреждением либо если Учреждение не вправе осуществлять обработку ПДн без согласия субъекта на основаниях, предусмотренных законодательством.

5.13.5. В случае отзыва субъектом согласия на обработку его ПДн Учреждение обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий 30 (тридцати) дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект, иным соглашением между Учреждением и субъектом, либо если Учреждение не вправе осуществлять обработку ПДн без согласия субъекта на основаниях, предусмотренных законодательством.

5.14. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в 5.13.3 - 5.13.5, Учреждение осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен законодательством.

Передача ПДн субъектов

5.15. При передаче ПДн субъекта представители Учреждения должны соблюдать следу-

ющие требования:

- не сообщать ПДн субъекта третьей стороне без письменного согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, а также в иных случаях, установленных законодательством;

- предупредить лиц, получающих ПДн субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн субъекта, обязаны соблюдать конфиденциальность. Данное положение не распространяется на обмен ПДн субъектов в порядке, установленном законодательством;

- разрешать доступ к ПДн субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн субъекта, которые необходимы для выполнения конкретных функций;

- осуществлять передачу ПДн в пределах Учреждения в соответствии с настоящей Политикой, иными локальными нормативными актами с которыми работники Учреждения должны быть ознакомлены под роспись;

- передача ПДн субъекта из Учреждения сторонним организациям осуществляется в объемах, необходимых для выполнения задач, соответствующих объективной причине сбора этих данных с соблюдением требований законодательства.

5.16. Учреждение вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено законодательством, на основании заключаемого с этим лицом договора (контракта). При этом лицо, осуществляющее обработку ПДн по поручению Учреждения, обязано соблюдать принципы и правила обработки ПДн, предусмотренные законодательством.

5.17. Лицо, осуществляющее обработку ПДн по поручению Учреждения, не обязано получать согласие субъекта ПДн на обработку его ПДн.

5.18. При передаче носителей, содержащих ПДн, составляется Акт приема-передачи.

Помещения, предназначенные для хранения и работы с ПДн субъектов

5.19. ПДн субъектов обрабатываются и хранятся в отделах Учреждения по направлениям деятельности. В целях выполнения своих служебных обязанностей ПДн субъектов могут обрабатываться сотрудниками Учреждения как на бумажных носителях, так и в электронном виде.

5.20. Размещение помещений, предназначенных для обработки ПДн субъектов и их оборудование должны исключать возможность бесконтрольного проникновения в эти помещения посторонних лиц и гарантировать сохранность находящихся в них носителей, содержащих ПДн.

5.21. Помещения, в которых обрабатываются ПДн субъектов, в рабочее время при отсутствии в них сотрудников должны быть закрыты.

Особенности обработки ПДн без использования средств автоматизации

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

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

5.24. 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, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

а) 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 (распространяется) копия ПДн;

б) при необходимости уничтожения или блокирования части ПДн уничтожается или бло-

кируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

5.25. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Учреждением.

6. ОБЕСПЕЧЕНИЕ ОБРАБОТКИ ПДн в ИСПДН

6.1. Учреждение при обработке ПДн обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн.

6.2. Порядок обработки ПДн в ИСПДн Учреждения регламентируется локальными нормативными актами Учреждения.

6.3. Автоматизированная обработка ПДн в ИСПДн осуществляется с применением методов защиты информации.

6.4. Обеспечение безопасности ПДн достигается, в частности:

1) определением угроз безопасности ПДн при их обработке в ИСПДн;

2) применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;

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

4) оценкой эффективности принимаемых мер по обеспечению безопасности ПДн;

5) учетом машинных носителей ПДн;

6) обнаружением фактов несанкционированного доступа к ПДн и принятием мер;

7) восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

9) контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

6.5. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям блоки с элементами накопления и хранения ПДн.

6.6. По фактам и попыткам несанкционированного доступа к ПДн, а также утечки ПДн проводятся служебные расследования.

7. СЛУЖЕБНЫЕ РАССЛЕДОВАНИЯ ПО ФАКТАМ РАЗГЛАШЕНИЯ ПДн, УТЕРИ НОСИТЕЛЯ(ЕЙ),СОДЕРЖАЩЕГО(ИХ) ПДн, И ИНЫХ НАРУШЕНИЙ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ

Создание комиссии

7.1. Разглашением ПДн субъекта(ов), является предание их огласке сотрудником, которому эти сведения были доверены для работы, в результате чего они стали известны третьим лицам.

7.2. Утерей носителя(ей), содержащего(их) ПДн субъекта(ов), является выход носителей из владения сотрудника, которому они были доверены для работы, в результате чего они стали либо могли стать известны третьим лицам.

7.3. За разглашение ПДн субъекта(ов), утерю носителя(ей), содержащего(их) ПДн субъекта(ов), а также за иные нарушения режима конфиденциальности виновные лица привлекаются к ответственности в соответствии с законодательством.

7.4. По факту разглашения ПДн субъекта(ов), утери носителя(ей), содержащего(их) ПДн субъекта(ов), организовывается служебное расследование и розыск носителя(ей), содержащего(их) ПДн субъекта(ов), а также принимаются меры по локализации возможного ущерба.

7.5. Для проведения служебного расследования руководитель Учреждения в день обна-

ружения факта разглашения ПДн субъекта(ов), утери носителя(ей), содержащего(их) ПДн субъекта(ов), приказом назначает комиссию из компетентных и не заинтересованных в исходе расследования сотрудников, не менее 3-х человек, имеющих допуск к ПДн субъектов. При необходимости указанные сотрудники освобождаются от исполнения своих должностных обязанностей на время проведения служебного расследования.

С приказом о создании комиссии необходимо ознакомить под роспись всех включенных в нее сотрудников.

7.6. Комиссия по ведению служебного расследования обязана:

- установить обстоятельства разглашения ПДн субъекта(ов), утери носителя(ей), содержащего(их) ПДн (время, место, способ и др.);
- провести обследование мест возможного нахождения утраченного носителя(ей), содержащего(их) ПДн субъекта(ов);
- определить актуальность утраченной (разглашенной) информации;
- вести розыск утерянного(ых) носителя(ей), содержащего(их) ПДн субъекта(ов);
- установить лиц, виновных в разглашении ПДн субъекта(ов), утере носителя(ей), содержащих ПДн субъекта(ов);
- установить причины и условия, способствующие разглашению ПДн субъекта(ов) и/или утере носителя(ей) ПДн субъекта(ов) и выработать рекомендации по их устранению;
- определить (произвести подсчет) ущерба (убытков).

7.7. При проведении служебного расследования члены комиссии имеют право:

- проводить осмотр помещений, хранилищ, столов, шкафов, в которых могут находиться носители, содержащие ПДн субъектов;
- проверять документацию, журналы учета и дела;
- затребовать объяснения от подозреваемых в проступке сотрудников, а при отказе в их представлении составить соответствующий акт;
- опрашивать сотрудников Учреждения, допустивших разглашение ПДн субъекта(ов), утерю носителя(ей) ПДн субъекта(ов), а также других сотрудников, могущих оказать содействие в установлении обстоятельств разглашения ПДн субъекта(ов), утери носителя(ей), содержащих ПДн субъекта(ов), и получать от них письменные объяснения.

7.8. Служебное расследование должно проводиться в предельно короткий срок (не более недели со дня обнаружения факта разглашения/утери).

7.9. В случае, если утерянные носители, содержащие ПДн субъекта(ов) не обнаружены, исчерпаны все возможные меры розыска, выяснены обстоятельства утери и установлены виновные в этом лица, розыск может быть прекращен.

Оформление результатов работы комиссии

7.10. Результаты работы комиссии отражаются в соответствующем акте.

7.11. По окончании служебного расследования комиссия обязана представить на рассмотрение руководителю Учреждения следующие документы:

- акт, содержащий результаты проведенного служебного расследования;
- письменные объяснения лиц, которых опрашивали члены комиссии;
- другие документы, имеющие отношение к служебному расследованию.

7.11.1. В акте должно быть отражено:

- фамилии и должности всех членов комиссии;
- дата, место и точное время составления акта;
- основание и время проведения расследования;
- сведения о проделанной работе;
- время, место и обстоятельства разглашения ПДн субъекта(ов) и/или утери носителя(ей), содержащих ПДн субъекта(ов);
- причины и условия совершения разглашения ПДн субъекта(ов) и/или утери носителя(ей), содержащих ПДн субъекта(ов);
- виновных лиц и степень их вины;
- размер причиненного ущерба и предложения по его возмещению;
- предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия.

Кроме того, в акте могут содержаться и другие сведения (напр., предложения по мерам,

которые необходимо принять для поиска конфиденциального документа или для недопущения подобных нарушений в дальнейшем).

7.12. Акт подписывается всеми членами комиссии. С ним необходимо ознакомить сотрудника, виновного в разглашении ПДн и/или утере носителя(ей), содержащего(их) ПДн субъекта(ов), под роспись. В случае его отказа или уклонения от ознакомления составляется соответствующий акт.

7.13. По результатам работы комиссии руководитель Учреждения принимает меры по локализации последствий разглашения ПДн субъекта(ов), утери носителя(ей), содержащего(их) ПДн субъекта(ов).

8. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ ОБРАБОТКИ ПДн

8.1. Каждый сотрудник, допущенный в установленном порядке к обработке ПДн, несет личную ответственность за конфиденциальность ПДн ставших ему известными.

8.2. Руководитель, разрешающий доступ сотрудника к ПДн, несет персональную ответственность за данное разрешение.

8.3. В случае нарушения законодательства в области защиты конфиденциальной информации сотруднику могут грозить:

- дисциплинарные взыскания (замечание, выговор, увольнение);
- отстранения от исполнения служебных обязанностей, связанных с доступом к ПДн субъектов;
- привлечения к материальной ответственности в рамках Трудового Кодекса Российской Федерации;
- привлечения к гражданско-правовой ответственности путем направления материалов в суд с иском о возмещении причиненного ущерба;
- привлечение к уголовной ответственности в соответствии с законодательством.

9. ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

9.1. Внутренний контроль соответствия обработки ПДн в Учреждении действующему законодательству и локальным нормативным актам Учреждения осуществляется с целью оценки фактического состояния обеспечения защиты ПДн, законности обработки ПДн, а также выявления недостатков и нарушений, выработки предложений, направленных на их устранение и предотвращение.

9.2. Внутренний контроль должен периодически проводиться ответственным за информационную безопасность в Учреждении. В случае необходимости внутренний контроль может проводиться комиссией, назначаемой приказом руководителя.