Приложение к приказу
от 29.12.2017г N 104

Правила обработки и хранения персональных данных в государственном бюджетном учреждении Балахнинский дом-интернат.

1. Термины и определения

В настоящих Правилах обработки персональных данных в государственном бюджетном учреждении Балахнинский дом-интернат (далее учреждение), устанавливающих процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, используются следующие термины и определения:

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

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющие обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

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

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

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

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

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

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

несанкционированный доступ к информации - неправомерное получение, использование, утрата, уничтожение, искажение, блокирование информации;

допуск к информации - официальное разрешение субъекту обращаться к информации определенного уровня конфиденциальности.

2. Перечень сокращений

ИСПДн	информационная система персональных данных
АРМ	автоматизированное рабочее место
ПДн	персональные данные
СрЗИ	средства защиты информации
СЗИ	система защиты информации

3. Общие положения

Целью Правил обработки персональных данных вУчреждении, устанавливающих процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее - Правила), является обеспечение прав и свобод человека и гражданина в отношении их персональных данных путем определения принципов, правил и методов защиты персональных данных от несанкционированного доступа, неправомерного их использования или утраты.

Правила определяют порядок обработки (включая сбор, хранение, передачу и любое иное использование) персональных данных в Учреждении(с использованием автоматизированного комплекса «VipNet» для защиты персональных данных получателей социальных услуг).

В Правилах не рассматриваются вопросы применяемых способов и методов защиты персональных данных.

Настоящий документ разработан в соответствии с требованиями следующих законодательных актов и нормативных документов:

- Конституции Российской Федерации;
- Гражданского кодекса Российской Федерации;
- Трудового кодекса Российской Федерации;
- Кодекса Российской Федерации об административных правонарушениях;

- Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных»;
- Федерального закона от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- постановления Правительства Российской Федерации от 17 ноября 2007г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- постановления Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства Российской Федерации от 21 марта 2012г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

4. Цели сбора, обработки и хранения персональных данных

Целью сбора, обработки и хранения персональных данных субъектов персональных данных в ИСПДн Учреждения является предоставление возложенных на Учреждение оказание стационарных социальных услуг.

5. Перечень персональных данных, обрабатываемых в Учреждении

Для осуществления возложенных на Учреждение функций обрабатываются следующие персональные данные:

Перечень персональных данных сотрудников:

- фамилия, имя, отчество;
- место, год и дата рождения;
- гражданство;
- адрес регистрации по месту жительства и проживания (фактический);
- паспортные данные (серия, номер паспорта, кем и когда выдан);
- информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- СНИЛС;
- информация о трудовой деятельности, трудовом стаже (место работы, должность, период работы, причины увольнения);

информация о состоянии здоровья;

- телефонный номер (домашний, мобильный);
- семейное положение и состав семьи;;
- должностной оклад;
- данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, условия труда, система оплаты);
- сведения о воинском учете (категория запаса, воинское звание, информация о снятии с воинского учета);
- ИНН;
- данные об аттестации работников;
- данные о повышении квалификации;
- данные о наградах, медалях, поощрениях, почетных званиях;
- информация о приеме на работу, перемещении, увольнении;
- информация об отпусках; информация о командировках;
- степень инвалидности.

Перечень персональных данных получателей социальных услуг:

- фамилия, имя, отчество;
- место, год и дата рождения;
- адрес регистрации по месту жительства и проживания (фактический);
- паспортные данные (серия, номер паспорта, кем и когда выдан);
- информация о трудовом стаже (место работы, должность, период работы, причины увольнения);
- адрес проживания (фактический);
- телефонный номер (домашний, рабочий, мобильный);
- семейное положение и состав семьи;
- сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- ИНН;
- данные о наградах, медалях, поощрениях, почетных званиях:
- степень инвалидности;
- информация о пенсионном обеспечении; информация о доходах
- СНИЛС;
- информация о состоянии здоровья;
- информация о судимости.

6. Принципы обработки персональных данных

При организации технологического процесса обработки персональных данных в ИСПДн Учреждения, сотрудники, допущенные к обработке ПДн должны руководствоваться следующими основными принципами:

- соблюдение законности целей и способов обработки ПДн;
- контроль достоверности ПДн и их достаточности для достижения заявленной цели;
- соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн;
- недопустимость обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн:
- соответствие объема, содержания и характера обрабатываемых ПДн, способа обработки ПДн целям обработки ПДн;
- соблюдение условий конфиденциальности ПДн в пределах взятых на себя обязательств, в соответствии с действующим законодательством Российской Федерации; ,
- исключение возможности обработки одного и того же массива ПДн в прикладных информационных системах (в том числе автоматизированных системах), различающихся по целевому назначению;
- обработка, хранение ПДн должны осуществляться в форме, позволяющей определить субъект ПДн, не дольше, чем этого требуют цели их обработки; по достижении цели обработки либо утраты необходимости в обработке ПДн подлежат уничтожению;
- безопасность информации.

7. Порядок обработки персональных данных

Порядок обработки персональных данных без использовании средств автоматизации

Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка персональных данных) может осуществляться в виде документов па бумажных носителях и в электронном виде (файлы, базы банных) на внешних носителях информации.

При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных (при необходимости получения письменного согласия на обработку персональных данных);
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

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

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление)

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных па том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

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

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации 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 персональными дан н ыми.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Правила обработки персональных данных средствами автоматизации

Обработка персональных данных средствами автоматизации в Учреждении допускается только в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации полномочий и обязанностей;
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);
- обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных услуг;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

,

- обработка персональных данных необходима для осуществления прав и законных интересов учреждения или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедос тупными субъектом персональных данных);

осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Обработка персональных данных средствами автоматизации должна осуществляться на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащих такие данные, определенный для выполнения конкретных операций с заранее определенными целями, с учетом требований настоящих правил.

Обработка персональных данных с согласия субъекта персональных данных

В случае если обработка персональных данных субъекта персональных данных в информационной системе персональных данных осуществляется на основании согласия и не имеется оснований для обработки таких персональных данных без получения согласия, должны выполняться указанные в настоящем пункте правила.

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку персональных данных должно быть:

- конкретным,

- информированным,
- сознательным.

Согласие на обработку персональных данных Учреждению может быть дано субъектом персональных данных или его представителем только в письменной форме.

Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Р.Ф.

В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяю тся оператором.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных или другие законные представители, если такое согласие не было дано субъектом персональных данных при его жизни.

В случае получения согласия от законного представителя субъекта персональных данных или наследников субъекта персональных данных они обязаны представить документы, пюдтверждающие их полномочия.

Допускается включение согласия в типовые формы (бланки) материальных носителей персональных данных и в договоры с субъектами персональных данных.

Письменные согласия субъектов персональных данных должны храниться вУчреждении. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных путем направления обращения вУчреждение.

Требования к содержанию согласия на обработку персональных данных приведено в настоящих і 1равилах.

Обработка персональных данных без согласии субъекта персональных банных

Обработка персональных данных, осуществляемая без получения согласия на такую обработку от субъекта персональных данных, может осуществляться только по основаниям, предусмотренным федеральным законом, при этом обязанность предоставить доказательство наличия таких оснований возлагается на Учреждение .

Правила исключительно автоматизированной обработки персональных данных

При исключительно автоматизированной обработке персональных данных должны выполняться правила обработки персональных данных средствами автоматизации.

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

В остальных случаях принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, запрещается.

При исключительно автоматизированной обработке персональных данных необходимо:

- разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных;
- разъяснить возможные юридические последствия такого решения;

- предоставить возможность заявить возражение против такого решения;
- рассмотреть возражение;
- уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

Правила смешанной обработки персональных данных

При смешанной обработке персональных данных необходимо выполнять правила, объединяющие правила обработки персональных данных при их обработке каждым из используемых при смешанной обработке персональных данных способов.

8. Порядок предоставления допуска и доступа к персональным данным

К работе с персональными данными, обрабатываемыми в ИСПДн Учреждения , должны допускаться только сотрудники, имеющие документально оформленный допуск к работе с ПДн.

Допуск к работе с персональными данными, обрабатываемыми в автоматизированном комплексе «VipNet оформляется после ознакомления сотрудника с должностной инструкцией (должностными обязанностями), с положениями Правил и подписания обязательства о неразглашении персональных данных, обрабатываемых в БД «VipNet».

Все лица, получившие доступ к персональным данным субъектов ПДн, обязаны не распространять их и не раскрывать их третьим лицам.

9. Порядок сбора персональных данных

Перед приемом документов с ПДн (началом работы с документами) от их обладателя (субъекта ПДн) сотрудник обязан предупредить обладателя документов о целях обработки ПДн о сроках их хранения в БД «VipNet», после чего может приступить к работе с ПДн субъекта.

10. Порядок использования персональных данных

Персональные данные субъектов ПДн используются в ИСПДн Учреждения в соответствии с пунктом 1 статьи 6 Федерального закона от 25 июля 2011г. № 152-ФЗ «О персональных данных», согласно которому обработка персональных данных осуществляется с согласия субъекта персональных данных.

Запрещается при обработке ПДн и ИСПДн Учреждения передавать ПДн в смежные автоматизированные системы (автоматизированные системы, различающиеся по целевому назначению) либо использовать полученные из смежных автоматизированных систем ПДн. В случае возникновения подозрений на неточность представленных, обрабатываемых, хранящихся ПДн необходимо осуществить блокирование персональных данных, если блокирование персональных данных не нарушает права и законные интересы субъекта ПДн или третьих лиц.

11. Порядок хранения персональных данных

Порядок хранения персональных данных в ИСПДн Учреждения должен исключать возможность утраты ПДн и/или их неправомерное использование.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных.

Сроки обработки и хранения ПДн в ИСПДн Учреждения определяются: достижением цели обработки ПДн; сроком исковой давности, а также иными требованиями законодательства Российской Федерации в части осуществления архивного хранения документов, образующихся в результате деятельности государственных органов, органов местного самоуправления и организаций.

Материальные носители, содержащие персональные данные, журналы учета материальных носителей должны храниться в рабочее и нерабочее время в металлических запирающихся шкафах, либо специально выделенных для храпения помещениях с регламентированным доступом.

Материальные носители информации выдаются для работы в начале дня исполнителям сотрудником, ответственным за их хранение, и в конце дня должны быть сданы и заперты в хранилище, которое опечатываться печатью ответственного за хранение материальных носителей.

12. Порядок уничтожении персональных данных

Уничтожение документов, содержащих ПДн, производится: по достижении целей их обработки согласно номенклатуре дел и документов; по достижении окончания срока хранения ПДн, оговоренного в соответствующем соглашении заинтересованных сторон; в том числе, если они не подлежат архивному хранению.

Уничтожение документов, содержащих персональные данные, производится в случае выявления неправомерной обработки персональных данных в срок, не превышающий десяти рабочих дней с момента выявления неправомерной обработки персональных данных.

Уничтожение информации с ПДн, хранящейся в электронном виде на материальных носителях, производится путем выполнения процедуры специальной подготовки материальных носителей (многократное форматирование разделов, выделенных под хранение данных).

Уничтожение материальных носителей с ПДн осуществляется механическим либо электромагнитным воздействием с помощью специализированных средств (шредер, уничтожитель оптических дисков и т.п.).

Уничтожение производится по мере необходимости в зависимости от объемов накопленных для уничтожения документов.

Для уничтожения материальных носителей и информации на материальных носителях документально создается экспертная комиссия в составе не менее 2 человек. Уничтожение осуществляется но акту.

Накапливаемые для уничтожения документы, копии документов, черновики, содержащие персональные данные, должны храниться отдельно.

13. Порядок восстановления персональных данных

Восстановление документов, содержащих персональные данные в ИСПДнУчреждения , осуществляется посредством программно-аппаратных средств ИСПДн Учреждения централизованно с автоматизированного рабочего места администратора ИСПДн Учреждения с применением дистрибутивов.

14. Порядок передачи персональных данных

При передаче персональных данных субъекта оператор должен соблюдать следующие требования:

- предупредить лиц, получающих персональные данные субъекта ПДн, 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 персональные данные субъекта ПДн, обязаны соблюдать режим конфиденциальности;
- разрешать доступ к персональным данным только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

Транспортировка, передача носителей персональных данных должна происходить в порядке, исключающем случайную утрату носителей или утечку персональных данных.

15. Основные меры (процедуры) препятствующие несанкционированному использованию персональных данных

Под процедурами, препятствующими несанкционированному использованию персональных данных, в целях реализации настоящего документа понимаются мероприятия по предупреждению

несанкционированного использования, оперативному и последующему контролю использования персональных данных, проводимые сотрудникамиУчреждения .

В Учреждении применяются следующие меры, препятствующие несанкционированному доступу к персональным данным:

ограничение доступа к персональным данным в специализированных программных средствах;

защита персональных данных при их обработке и архивировании; ограничение доступа посторонних лиц в помещения учреждения, предназначенные для осуществления работы с ПДн;

защита рабочих мест работников, осуществляющих операции с программными средствами;

контроль за соблюдением работниками учреждения требований законодательства РФ н иных нормативных правовых актов.

В целях противодействия несанкционированному использованию персональных данных, предотвращения утечки и обеспечения сохранности персональных данных в Учреждении используется следующий комплекс мероприятий:

ограничение доступа к служебной информации в программных средствах:

обеспечение доступа к данным только в пределах полномочий, представленных непосредственно исполнителям, обеспечивающим ведение, обработку и учет информации с ПДн;

установление индивидуальных кодов и паролей доступа к данным для каждого исполнителя;

осуществление административных и технических мер, направленных на исключение несанкционированного доступа к данным: блокирование доступа пользователя в систему в случае обнаружения попыток несанкционированного доступа, установка программных средств, оповещающих ответственного за организацию работы по обеспечению защиты информации о попытке несанкционированного доступа, блокировка рабочего места нарушителя;

контроль за соблюдением режима обращения персональных данных осуществляется ответственным за организацию работы по обеспечению защиты информации, а также директором учреждения.

1. *защита персональных данных при ее обработке и архивировании:*

обеспечение дублирования данных в процессе их ввода, предусматривающее сохранность первичного носителя информации;

установка программных средств для создания резервных копий, способствующих быстрому восстановлению данных;

использование систем защиты информационно-технических систем и каналов связи от утечки персональных данных;

осуществление резервного копирования (восстановления) только уполномоченными сотрудниками.

2. *ограничение доступа посторонних лиц в помещения учреждения, предназначенные для осуществления сбора, обработки и хранения информации ПДн, осуществляются за счёт:*

- соблюдения порядка и правил доступа в служебные помещения в соответствии с положением о защите ПДн в учреждении, утвержденном директором;
- ограничения доступа работников и посторонних лиц в помещение, в котором размещены персональные компьютеры, вычислительные системы и системы телекоммуникаций для осуществления операций с ПДн.
- защита рабочих мест работников, осуществляющих сбор и обработку ПДн:

защита окон в служебных помещениях от внешнего дистанционного наблюдения жалюзи и шторами;

эффективное размещение рабочих мест сотрудников для исключения возможности несанкционированного просмотра документов и информации на мониторах;

соблюдение сотрудниками подразделений правил по обеспечению защиты информации при работе с персональными компьютерами.

5. *ограничение доступа к персональным данным:*

доступ работников к необходимым документам только для выполнения своих служебных обязанностей;

проведение инвентаризации мест хранения документов, содержащих персональные данные;

контроль за соблюдением утвержденных внутренних регламентов.

При оформлении на работу в учреждение работник дает расписку о неразглашении персональных данных.

Контроль за соблюдением работниками учреждения требований законодательства РФ и иных нормативных правовых актов, регулирующих работу с ПДн, внутренними документами Учреждения возложен на директора.

16. Порядок действий при обнаружении фактов несанкционированного доступа к персональным данным и принятие мер

В случае обнаружения фактов несанкционированного доступа к ПДн, обрабатываемым в программно-аппаратных средствах ИСПДн Учреждения , администратор безопасности должен предпринять следующие меры:

-отключить конкретное программно-аппаратное средство ИСПДн Учреждения (АРМ. сервер, телекоммуникационное оборудование), к которому совершен несанкционированный доступ;

- проанализировать тестовые сообщения, предусмотренные в программно-аппаратных средствах ИСПДн Учреждения или провести анализ состояния предусмотренных производителем индикаторов и электронных протоколов устройств для телекоммуникационного оборудования;
- по возможности устранить неисправность путем использования эталонных дистрибутивов и эксплуатационной документации на программно-аппаратные средства ИСПДнУчреждения .

В случае обнаружения фактов несанкционированного доступа в помещения, где обрабатываются ПДн. к сейфовым шкафам, предназначенным для хранения ПДн, к материальным носителям, содержащим ПДн, ответственное лицо по защите информации на объекте информатизации должно провести должностное расследование по факту несанкционированного доступа с целью выявления нарушителя.

17. Правила рассмотрения запросов субъектов персональных данных или их представителей

Субъект персональных данных имеет право требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

В соответствии с Федеральным законом от 27 июля 2006г. № 152-ФЗ «О персональных данных» в случае поступления обращения от субъекта ПДн в устной форме либо в форме письменного запроса Учреждения обязан предоставить сведения, касающиеся обработки его ПДн, в том числе:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

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

- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его ПДн.

Изложенные выше сведения должны быть представлены субъекту ПДн в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Запрос о предоставлении ПДн должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя. Письменный запрос может быть направлен в электронной форме (в форме электронного документа, подписанного юридически значимой электронной цифровой подписью в соответствии с законодательством Российской Федерации); запрос, поступивший в электронном виде, принимается к рассмотрению в случае валидности электронной цифровой подписи, которой подписан документ.

Ответ на письменный запрос субъекта ПДп, поступивший в электронной форме, может быть направлен по электронному адресу субъекта ПДн при выполнении следующих условий:

- ответ не содержит сведения ограниченного распространения (конфиденциальную информацию, в том числе ПДн);
- ответ подписан электронной цифровой подписью сотрудника в соответствии с законодательством Российской Федерации;
- субъект ПДн не возражает против такой формы предоставления информации (субъект предоставил письменное подтверждение о готовности принять информацию по указанному им электронному адресу).

Во всех остальных случаях ответ на письменный запрос может быть направлен в адрес субъекта ПДн через почтовую связь только в форме документа на бумажном носителе, в специальном конверте, не позволяющем просмотреть содержание документа без его вскрытия.

В предоставлении ПДп по запросу субъекта ПДн может быть отказано в случаях, предусмотренных в пункте 6 статьи 14 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных», а также в случае поступления запроса в электронной форме, подписанного электронной цифровой подписью, достоверность которой не подтверждается в результате выполнения проверки. В том и в другом случаях оператор обязан уведомить субъекта ПДн о причине отказа.

18. Правила осуществлении внутреннего контроля

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в ИСПДн в Учреждении организуется проведение периодических проверок условий обработки персональных данных, в соответствие установленным графиком.

Проверки осуществляются ответственным за организацию обработки персональных данных в ИСПДн Учреждения либо комиссией, создаваемой распоряжением директораУчреждения .

В проведении проверки не могут участвовать сотрудники, прямо или косвенно заинтересованные в её результатах.

Проверки соответствия обработки персональных данных установленным требованиям проводятся в ИСПДн в Учреждении проводятся на основании утвержденного директором ежегодного плана мероприятий по организации защиты персональных данных или па основании поступившего в Учреждение письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне исследованы:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных и обеспечения установленных уровней защищенности персональных данных;
- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- мероприятия но восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа;
- осуществление мероприятий по обеспечению целостности персональных данных.

Ответственный за организацию обработки персональных данных в ИСПДн Учреждения (член комиссии) имеет право:

- запрашивать у сотрудников, обрабатывающих персональные данные в ИСПДнУчреждения , информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных должностных лиц у точнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в сфере обработки персональных данных.

В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в ИСПДн Учреждения (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться их конфиденциальность.

Проверка должна быть завершена не позднее, чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, директору докладывает в форме письменного заключения ответственный за организацию обработки персональных данных либо председатель комиссии.

Директор, назначивший внеплановую проверку, обязан контролировать своевременность и правильность её проведения.

19. Акты уничтожении персональных данных и иной конфиденциальной информации, находящихся на программно-технических средствах комплексов средств автоматизации

УТВЕРЖДАЮ
(должность руководителя)

АКТ
УНИЧТОЖЕНИЯ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Комиссия, наделенная полномочиями в соответствии с приказом _____
от _____ № _____ в составе: (должности. ФИО),
провела отбор документов, содержащих персональных данные, не подлежащих дальнейшему хранению:

№	Дата документа	Учетный помер документа	Заголовок (краткое содержание)	Номера описей дела	1рнмечанис
1	т	Ч	4	5	6

Всего документов _____ на
_____ листах
(цифрами и прописью) (цифрами и прописью)
Перечисленные документы уничтожены путем измельчения на специальной бумагорезательной машине (шредере) _____
(Дата)

Председатель комиссии:
(ФИО) Подпись Дата

Члены комиссии:
(ФИО) Подпись Дата

(должность, ФИО) (должность, ФИО)

Председатель комиссии: Члены комиссии:

УТВЕРЖДАЮ
Директор
(Ф.И.О., подпись 200_ г.

АКТ

уничтожения персональных данных и иной конфиденциальной информации, находящейся на программно-технических средствах комплексов Учреждения
от " "_____20 г.

Системный администратор: _____ (должность, ФИО)
составили настоящий акт в том, ч то " ___ " _____ 20_ г. произведено уничтожение персональных данных или иной конфиденциальной информации, находящейся на
(наименование АРМ по утвержденной конфигурации, ФИО ответственного пользователя АРМ, заводской или учетный номер системного блока ПЭВМ, носителя информации, тип удаляемой конфиденциальной информации в соответствии с утвержденным перечнем персональных данных и иной конфиденциальной информации, способ уничтожения информации).

Председатель комиссии: _____(подпись)

Члены комиссии: _____(подпись)

Системный администратор: _____ (подпись)

Примечание. Комиссия должна назначаться приказом директора и состоять не менее чем из двух человек, допущенных к работе с персональными данными н иной конфиденциальной информацией.

20. Порядок доступа сотрудников Учреждения к помещениям, в которых ведется обработка персональных данных

Общие положения

Настоящий Порядок разработан в целях обеспечения безопасности персональных данных при их обработке (в том числе хранении) путем создания условий, затрудняющих несанкционированный доступ к техническим средствам, участвующим в обработке персональных данных, и материальным носителям персональных данных, а также обеспечения внутри объектового режима.

Объектами охраны Учреждения являются помещения, в которых происходит обработка персональных данных, как с использованием средств автоматизации, так и без таковых;

- помещения, в которых установлены компьютеры, серверы, участвующие в обработке персональных данных;
- помещения, в которых хранятся материальные носители персональных данных;
- помещения, в которых хранятся резервные копии персональных данных.

Бесконтрольный доступ посторонних лиц в указанные помещения должен быть

исключен.

Ответственность за соблюдение настоящего Порядка несут сотрудники структурных подразделений, обрабатывающих персональные данные, а также руководители структурных подразделений.

Контроль за соблюдением требований настоящего Порядка обеспечивает специалист по информационной безопастности.

Все объекты охраны должны предусматривать круглосуточное дежурство, а также предполагать существенные трудности для нарушителя по их преодолению: металлические решетки на окнах на первом этаже здания.

Доступ в помещении, в которых ведется обработки персональных данных

Доступ посторонних лиц в помещения, в которых ведется хранение и обработка персональных данных, должен осуществляться только ввиду служебной необходимости.

При этом на момент присутствия посторонних лиц в помещении должны быть приняты меры по недопущению ознакомления посторонних лиц с персональными данными. Пример: мониторы повернуты в сторону от посетителей, документы убраны в стол либо находятся в непрозрачной папке (накрыты листами бумаги).

Допуск сотрудников в помещения, в которых ведется обработка и хранение персональных данных, оформляется после подписания сотрудником обязательства о неразглашении и инструктажа ответственного за информационную безопасность.

В нерабочее время помещения, в которых ведется обработка персональных данных, должны находиться под охраной, при этом все окна и двери должны быть надежно закрыты, компьютеры выключены и заблокированы.

21. Типовая форма согласия на обработку персональных данных

СОГЛАСИЕ

на обработку персональных данных

Я _____
(ФИО)
проживающий(ая) по адресу: _____
паспорт _____ , выданный _____

(серия,номер) (кем выдан)

(место выдачи паспорта)

даю согласие оператору персональных данных:ГБУ Балахнинский дом-интернат , расположенному по адресу: г. Балахна, пр.Революции, д.85 на обработку:

Персональные данные, в отношении которых дается согласие Нужное отмети ть знаком "V"

моих персональных данных (дается заявителем)

персональных данных моего ребенка (детей) (дается заявителем)
I

в целях
в соответствии с действующим законодательством.

Персональные данные, в отношении которых дается настоящее согласие, включают данные, указанные в настоящем согласии, заявлении и представленных заявителем (представителем заяви теля) документах (фамилия, имя, отчество; дата рождения: пол; данные субъекта РФ (республики СНГ); индекс, почтовый адрес; контактный телефон.

Действия с персональными данными включают в себя их обработку (сбор, запись, и систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ),
обезличивание, блокирование, удаление, уничтожение).

Обработка персональных данных: автоматизированная (с использованием средств вычислительной техники) либо без использования средств автоматизации. Согласие действует с момента его подачи до моего письменного отзыва данного согласия.

« _____ » _____ 20 _____ г. _____
(дата) (подпись)

22. Типовая форма отзыва согласия на обработку персональных данных

В ГБУ Балахнинский дом-интернат
От_____
проживающей(его) но
адрес у:
паспорт серия №_____
выданный_____

Заявление

Прошу Вас прекратить обработку
Персональные данные, в отношении которых дается отзыв согласия : Нужное отметить знаком "V"

моих персональных данных
(дается заявителем)
персональных данных моего ребенка (детей)
(дается заявителем)
в связи

_____
(указать причину)

Мне известно, что в случае отзыва мною данного согласия (в период его действия), гражданско-правовые отношения с Учреждением буду прекращены.
" _____ " _____ 201 __ г. _____ _____
(подпись) (расшифровка подписи)

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

Уважаемый (ая)_____
(Ф.И.О)
в соответствии с требованиями Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных установлена _____

В случае отказа Вами предоставить свои персональные ,ГБУ Балахнинский дом-интернат не сможет на законных основаниях осуществлять обработку Ваших персональных данных, что приведет к следующим для Вас юридическим последствиям:

- непредоставление мер социальной поддержки, предусмотренных действующим законодательством;

всоответствии с действующим законодательством Российской Федерации в области персональных данных Вы имеете право:

- на получение сведений о наличии в Учреждении своих персональных данных, а также на ознакомление е такими персональными данными;

требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- обжаловать действия или бездействия Учреждения в уполномоченный орган но защите прав субъектов персональных данных в судебном порядке;

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

С разъяснениями ознакомлен(а) _____
(Ф.И.О.)
Подпись
Дата

24. Типовое обязательство работника ГБУ Балахнинский дом-интернат», непосредственно осуществляющего обработку персональных данных, о прекращении обработки персональных данных в случае расторжения трудового договора

Директору_____

(фамилия, имя, отчество, должность)

Я,_____обязуюсь прекратить обработку персональных данных, ставших известными мне

в связи с

исполнением должностных обязанностей, в случае расторжения со мной трудового договора, освобождения меня от замещаемой должности и увольнения с работы. В соответствии со статьей 7 Федерального закона от 27 июля 2006г № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются информацией ограниченного доступа и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная Федеральным законом от 27 июля 2006г. № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснена.

«___» _____ 20__ года _____
(подпись)