Приложение 1
к приказу УСЗН г. Дзержинска
от 31.12.2013 г. № 86-ОД

Положение по обеспечению безопасности персональных данных при их обработке в ИСПДн.

1. Общие положения

1.1. Целью настоящего Положения является обеспечение безопасности объектов информационной системы оператора от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационной системы.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.2.Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

1.3.В Положении определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн оператора. Назначение ответственного за организацию обработки персональных данных.

1.4.Применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с законодательством.

Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

1.5.Управление социальной защиты населения г. Дзержинска (далее – Управление) обеспечивает неограниченный доступ к документу, определяющему его Положение в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных, путем размещения на официальном сайте.

2. Основные понятия и правила обработки персональных данных:

2.1. Для реализации Положения используются следующие основные понятия:

1**) персональные данные** - любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
2) **оператор** – Министерство социальной политики Нижегородской области самостоятельно или совместно с другими лицами организует и (или) осуществляет обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
3) **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;
4) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;
5) **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
6) **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
7) **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;
8) **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
9) **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационными технологиями и техническими средствами;
10) **конфиденциальность персональных данных** - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;
11) **субъект** - гражданин Российской Федерации и иностранный гражданин, постоянно и временно проживающий на территории Нижегородской области, а также гражданин, состоящий в трудовых отношениях с оператором в соответствии с законодательством.

2.2. Обработка ПДн оператором осуществляется в соответствии с :
1. Федеральным законом Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных»;

2. Указом Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
3. Постановлением Правительства Российской Федерации от 21.03.2012 г. № 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. Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
5. Положение об обработке персональных данных в министерстве социальной политики Нижегородской области № 284 от 26.03.2013

2.3 Область действий:

Требования настоящего Положения распространяются на всех сотрудников.

2.4. Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

- перечня персональных данных, подлежащих защите;
- модели угроз безопасности персональных данных;
- разграничение прав доступа к обрабатываемым персональным данным;
- руководящих документов ФСТЭК и ФСБ России.

2.5. Управление осуществляет обработку следующих ПДн на:

1) граждан РФ и иностранных граждан, постоянно и временно проживающих на территории, лиц без гражданства на территории Нижегородской области (фамилия, имя, отчество, пол, дата рождения, адрес регистрации, место работы, серия и номер паспорта или документа удостоверяющего личность), обратившихся в Управление;

2.6. Цели обработки ПДн Управлением:

1) ведение учета обратившихся граждан за мерами социальной поддержки;
2) формирование системы учета и отчетности и иных информационных ресурсов в сфере социальной защиты населения в Российской Федерации;
3) предоставление данных организациям по соглашениям и возложенным на них государственным функциям.

2.7. Категории ПДн, обрабатываемых в ИСПДН:

- граждане Российской Федерации и иностранные граждане, постоянно и временно проживающие на территории Нижегородской области. По критериям:

- фамилия, имя, отчество;
- место, год и дата рождения;
- адрес по прописке;
- паспортные данные (серия, номер паспорта, кем и когда выдан);

- информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
- адрес проживания (реальный);
- телефонный номер (домашний, рабочий, мобильный);
- семейное положение и состав семьи (муж/жена, дети);
- данные о удостоверениях, наградах, медалях, поощрениях, почетных званиях;
- степень инвалидности;

2.8. Обработка ПДн осуществляется путем смешанной обработки ПДн с использованием информационной системы ПДн (далее - ИСПДн). Полученные в ходе обработки информации данные передаются:
1) по внутренней сети, с разграничением прав доступа сотрудников Управления;
2) по защищенным каналам связи или на внешних носителях информации для обмена информацией конфиденциального характера между управлениями и Министерством социальной политики Нижегородской области;
3) по каналам факсимильной связи для приема и передачи служебной информации;
4) по сети общего пользования «Интернет» только статистические и отчетные данные;

2.9. Сроки или условия прекращения обработки ПДн.

Основанием для прекращения обработки ПДн является: прекращение деятельности оператора, изменение действующего законодательства Российской Федерации, другие предусмотренные законодательством Российской Федерации и Нижегородской области основания.

3. Правила рассмотрения запросов субъектов ПДн или их представителей:

3.1. Субъект ПДн имеет право на получение сведений, касающихся обработки его ПДн. Сведения предоставляются субъекту ПДн или его представителю Управления при обращении либо при получении запроса субъекта ПДн или его представителя.
Субъект ПДн вправе требовать от Управления социальной защиты населения уточнения его 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.
3.2. Запрос, направленный в форме электронного документа должен быть подписан электронной подписью в соответствии с законодательством Российской Федерации.
Запросы, не отвечающие указанным требованиям не подлежат обработке, в соответствии с федеральным законодательством.
3.3. Сведения должны быть предоставлены субъекту ПДн Управления в доступной форме. В них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

4. Правила осуществления внутреннего и внешнего контроля соответствия обработки ПДн и требования к защите ПДн:

4.1. Порядок внутреннего контроля над соблюдением требований по обработке и обеспечению безопасности данных.

С целью соблюдения законности обработки и обеспечения безопасности ПДн Управлением проводится периодический контроль над соблюдением установленных требований.

Контроль над исполнением нормативных актов оператора по вопросам обработки и обеспечения безопасности ПДн возлагается на ответственного за организацию обработки ПДн, назначаемого приказом директора Управления.

Основными вопросами внутреннего контроля соответствия обработки ПДн являются:

1) соответствие документации по вопросам обработки ПДн реальному положению дел;

2) соблюдение сотрудниками, допущенными к обработке ПДн, всех требований установленных локальными нормативными актами оператора и Управления.

3) проверка соблюдения защиты прав субъектов ПДн, путем анализа их обращений и действий, совершаемых сотрудниками Управления, в связи с этими обращениями.

4.2. Порядок внешнего контроля за соблюдением требований по обработке и обеспечению безопасности персональных данных.

Законодательство в области ПДн определяет следующие контролирующие органы по вопросам обработки и обеспечения безопасности ПДн:

1) федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи является уполномоченным органом по защите прав субъектов ПДн, на который возлагается обеспечение контроля и надзора за соответствием обработки ПДн требованиям законодательства в области ПДн.

2) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации осуществляют контроль и надзор за выполнением требований:

- к обеспечению безопасности ПДн при их обработке в информационных системах ПДн;
- к материальным носителям ПДн и технологиям хранения таких данных вне информационных систем ПДн в пределах их полномочий и без права ознакомления с ПДн, обрабатываемыми в информационных системах ПДн.

4.3. Порядок проведения контроля устанавливается уполномоченным органом. При этом, уполномоченный орган по защите прав субъектов ПДн имеет право:

1) запрашивать информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

2) осуществлять проверку сведений, содержащихся в уведомлении об обработке ПДн или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;
4) принимать в установленном законодательством Российской Федерации и Нижегородской области порядке меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства;
5) обращаться в суд с исковыми заявлениями в защиту прав субъектов ПДн, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов ПДн в суде;
6) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области контроля и надзора в сфере информационных технологий и связи, применительно к сфере их деятельности, сведения, указанные в п.п. 5,7.1,10 и 11 части 3 статьи 22 Федерального закона от 27.07.2006 №152-ФЗ «О ПДн»;
7) направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн, в соответствии с подведомственностью;
8) привлекать к административной ответственности лиц, виновных в нарушении законодательства в области ПДн.

Решения уполномоченного органа по защите прав субъектов ПДн могут быть обжалованы в судебном порядке.

4.4. Правила работы с обезличенными ПДн :

Под обезличиванием ПДн понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Обезличивание ПДн Управлением при обработке ПДн с использованием средств автоматизации может осуществляться с целью выполнения требований по предоставлению отчетности по результатам деятельности в соответствии с нормативными документами органов государственной власти и оператором, а также в связи с достижением целей обработки ПДн.

Допускается обезличивание ПДн при обработке ПДн без использования средств автоматизации производить способом, исключающим дальнейшую обработку этих ПДн, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

5. Перечень информационных систем ПДн.

№ п/п	Наименование информационных систем, баз и банков данных, реестров, регистров, номенклатур дел	Область применения, описание	Категория содержащейся информации (для открытого доступа/ ограниченного доступа)
1	Информационная система Социальной защиты населения	Комплекс «Соцпомощь»	Для ограниченного доступа
2	Информационная система централизованной бухгалтерии, кадры	Система автоматизации бухгалтерского и кадрового учета	Для ограниченного доступа

6. Пользователи ИСПДн

6.1. В Положении Управления в отношении обработки и информационной безопасности ПДн определены основные категории пользователей. На основании этих данных производится типизация пользователей ИСПДн, определен их уровень доступа и возможности.

6.2. В ИСПДн Управления можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора БД;
- Администратора безопасности;
- Пользователи АРМ;

6.3. Данные о группах пользователей, уровне их доступа и информированности отражены в картах доступа к обрабатываемым персональным данным. (Приложение 2)

6.4. Администраторы БД, безопасности, обеспечивают функционирование подсистемы управления доступом ИСПДн и уполномочены осуществлять предоставление и разграничение доступа конечного пользователя к элементам, хранящим персональные данные.

6.5. Администраторы БД, безопасности обладают следующим уровнем доступа и знаний:
- полной информацией о системном и прикладном программном обеспечении ИСПДн;
- полной информацией о технических средствах и конфигурации ИСПДн;
- правами конфигурирования и административной настройки технических средств ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.

6.6. Администратор безопасности, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской части.

6.7. Администратор безопасности обладает:
- правами Администратора БД;
- полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.

6.8. Администратор безопасности уполномочен:

- реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты.

6.9. Оператор АРМ, осуществляющий обработку ПДн.

Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

6.10. Пользователь ИСПДн:
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

7. Обязательство о неразглашении ПДн, непосредственно осуществляющего обработку ПДн.:

7.1. Обязательство, осуществляющего обработку ПДн оператора подписывается сотрудником.
7.2. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку по своей воле для своих интересов и сознательно. Согласие на обработку ПДн должно быть конкретным.

Согласие на обработку ПДн может быть отозвано субъектом ПДн.
7.3. Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя:
1) фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и наименование выдавшего органа;
2) фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и наименование выдавшего органа, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);
3) фамилию, имя, отчество и наименование органа (Управления социальной защиты г.Дзержинска), получающего согласие субъекта ПДн;
4) цель обработки ПДн;
5) перечень ПДн, на обработку которых дается согласие субъекта Пдн в соответствии с законодательством.
6) подпись субъекта ПДн.

8. Требования к персоналу по обеспечению защиты ПДн:

8.1. Все сотрудники Управления, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.
8.2. При вступлении в должность нового сотрудника, допущенного к работе с персональными данными обрабатываемыми в информационной системе, ответственный за проведение первичного инструктажа обязан организовать его ознакомление с программой первичного инструктажа и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.
8.3. Сотрудник должен быть ознакомлен с настоящим Положением и принятых процедурах работы с элементами ИСПДн и СЗПДн.
8.4. Сотрудники Управления, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.
8.5. Сотрудники отдела автоматизации и информационного обслуживания должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).
8.6. Сотрудники отдела автоматизации и информационного обслуживания должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.
8.7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.
8.8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами оператора, третьим лицам.
8.9. При работе с ПДн в ИСПДн сотрудники Управления обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ.
8.10. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ с помощью блокировки ключом или эквивалентного средства контроля, доступом по паролю, если не используются более сильные средства защиты.
8.11. Сотрудники должны быть проинформированы ответственным по обеспечению безопасности ПДн в ИСПДн об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятую политику и процедуры безопасности ПДн.

8.12. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

9. Порядок доступа в помещения, в которых ведется обработка ПДн:

Запретить допуск посторонних лиц в кабинеты, в которых расположены технические средства ИСПДн, во время обработки персональных данных. В случае приема в кабинетах посторонних лиц обработка персональных данных должна производиться таким образом, чтобы исключить просмотр посторонними лицами текстовой и графической видовой информации отображаемой устройствами отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн.

10. Правовые, организационные и технические меры для обеспечения установленных уровней защищенности ПДн.

10.1. В соответствии со штатным расписанием организованы отделы для обработки ПДн.
11.2. Приказом по УСЗН назначены ответственные:

- за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных (администратором безопасности);
- за организацию обработки ПДн (Администратор БД).

10.3. Для каждого структурного подразделения предусмотрены следующие организационные и технические меры для обеспечения установленных уровней защищенности ПДн:
1) Разработаны и утверждены директором Управления Положения об отделах и должностные инструкции сотрудников, осуществляющих обработку ПДн.
2) Заключены обязательства о неразглашении ПДн с сотрудниками, осуществляющими обработку ПДн.
3) Определен перечень должностей работников, имеющих доступ к персональным данным в ИСПДН и осуществляющих их обработку в Управлении (Приложение 3).

11. Обработка ПДн без использования средств автоматизации (неавтоматизированная обработка ПДн):

11.1. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем

фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).
11.2. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, должны соблюдаться следующие условия:
1) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры, журналы и др.);
2) обработка ПДн, осуществляется таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.
3) необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.
4) при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

12. Осуществление внутреннего контроля соответствия обработки ПДн.

Внутренний контроль соответствия обработки ПДн проводится ежегодно.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывает директору управления ответственный за обеспечение безопасности в ИСПДн.

13. Принятые сокращения:

ПДн – персональные данные;

ИСПДн – информационные системы персональных данных;

СЗПДн – система защиты персональных данных;

УБПДн – угрозы безопасности персональных данных;

БД – база данных;

НСД – настройка системы данных.