Утверждено
Приказом директора
ОГБУ «Поназыревский КЦСОН»
№ 186 от 23 ноября 2026 г.

ПОЛОЖЕНИЕ

ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ОГЛАВЛЕНИЕ

1. ТЕРМИНЫ И СОКРАЩЕНИЯ 3

2. ОБЛАСТЬ ПРИМЕНЕНИЯ.....4

3. ОБЩИЕ ПОЛОЖЕНИЯ 5

4. ОРГАНИЗАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДн 6

5. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДн 8

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

Персональные данные (ПДн) – 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 ПДн – 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 ПДн – обработка ПДн с помощью средств вычислительной техники.

Распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Блокирование ПДн – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

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

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Положение об обеспечении безопасности ПДн (далее – Положение) разработано в целях выполнения требований законодательства Российской Федерации в области защиты ПДн.

2.2. Настоящее Положение определяет порядок и правила организации и проведения работ по обеспечению безопасности ПДн в **Областном государственном бюджетном учреждении «Поназыревский комплексный центр социального обслуживания»** (далее – Оператор).

2.3. Настоящий документ учитывает положения основных нормативных правовых актов в области защиты ПДн, перечисленных в Положении о комиссии по приведению в соответствие с требованиям законодательства в области ПДн.

2.4. Настоящее Положение предназначено для всех работников Оператора, а также третьих лиц, получающих временный или постоянный доступ к обрабатываемым у него ПДн на законном основании.

2.5. Настоящее Положение действует с момента его утверждения руководителем Оператора.

Актуализация настоящего Положения проводится не реже, чем два раза в год в соответствии с Регламентом по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности в **Error! Reference source not found.** Внесение изменений в настоящее Положение либо утверждение его новой редакции производится на основании соответствующего приказа руководителя Оператора.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. ПДн, обрабатываемые у Оператора, цели, основание и сроки их обработки указаны в Перечне обрабатываемых ПДн.

3.2. Обработка ПДн осуществляется Оператором с использованием средств автоматизации и без их использования.

3.3. Сроки хранения ПДн устанавливаются в письменном согласии субъекта ПДн на обработку его ПДн, а также требованиями законодательства Российской Федерации, устанавливающими сроки хранения документов.

4. ОРГАНИЗАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДн

4.1. Под организацией работ по обеспечению безопасности ПДн понимается формирование и всестороннее обеспечение реализации совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию как непосредственного, так и опосредованного ущерба от реализации угроз безопасности ПДн, и осуществляемых в целях:

- предотвращения возможных (потенциальных) угроз безопасности ПДн;
- нейтрализации и/или парирования реализуемых угроз безопасности ПДн;
- ликвидации последствий реализации угроз безопасности ПДн.

4.2. Организация работ по обеспечению безопасности ПДн у Оператора должна осуществляться в соответствии с действующими нормативными правовыми актами и разработанными для этих целей организационно-распорядительными документами по обеспечению безопасности ПДн Оператором.

4.3. Задачи по приведению деятельности Оператора в соответствие с требованиями законодательства Российской Федерации в области ПДн возлагаются на специально создаваемую для этих целей Комиссию и лиц, ответственных за организацию обработки и обеспечение безопасности ПДн, которые могут быть включены в состав данной Комиссии.

4.4. В случаях, когда Оператор на основании договора поручает обработку ПДн третьему лицу, Оператору необходимо заключить с данным лицом соглашение о соблюдении безопасности ПДн, с возложением на третье лицо обязанности по обеспечению конфиденциальности и безопасности переданных Оператором ПДн (либо включить данное обязательство в заключаемый/действующий договор).

4.5. Работы по приведению деятельности Оператора в соответствие с требованиями законодательства Российской Федерации ведутся по двум направлениям: обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, и обеспечение безопасности ПДн в ИСПДн Оператора.

4.6. Работы по обеспечению безопасности ПДн, обрабатываемых без использования средств автоматизации, ведутся по следующим направлениям:

- определение перечня лиц, допущенных к обработке ПДн;
- определение помещений, в которых обрабатываются ПДн;

- информирование работников Оператора об установленных правилах обработки ПДн и требований по их защите, повышение осведомленности в вопросах обеспечения безопасности ПДн;
- учет и защита носителей ПДн;
- разграничение доступа к носителям ПДн;
- уничтожение ПДн.

4.7. Организация и выполнение мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн Оператора, осуществляются в рамках системы защиты персональных данных ИСПДн (далее - СЗПДн), развертываемой в ИСПДн в процессе ее создания или модернизации.

4.8. СЗПДн представляет собой совокупность организационных мер и технических средств защиты информации, а также используемых в ИСПДн информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности ПДн.

4.9. СЗПДн должна являться неотъемлемой составной частью каждой вновь создаваемой ИСПДн Оператора.

4.10. Для существующих ИСПДн, в которых в процессе их создания не были предусмотрены меры по обеспечению безопасности ПДн должен быть проведен комплекс организационных и технических мероприятий по разработке и внедрению СЗПДн.

4.11. Структура, состав и основные функции СЗПДн определяются в соответствии с уровнем защищенности ПДн, обрабатываемых в ИСПДн и моделью угроз безопасности ПДн при их обработке в ИСПДн.

5. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДн

5.1. В целях оценки уровня защищенности, обрабатываемых у Оператора ПДн, и своевременного устранения несоответствий требованиям законодательства РФ в области защиты ПДн у Оператора раз в год должен проводиться анализ изменений процессов защиты ПДн.

5.2. Анализ изменений проводится по следующим основным направлениям:

- перечень должностей и третьих лиц, имеющих доступ к ПДн, степень их участия в обработке ПДн и характер взаимодействия между собой;
- перечень помещений для обработки ПДн;
- перечень и объем обрабатываемых ПДн;
- цели обработки ПДн;
- процедуры сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожение ПДн;
- способы обработки ПДн (автоматизированная, неавтоматизированная);
- перечень уполномоченных органов, в рамках отношений с которыми осуществляется обработка ПДн;
- перечень программно-технических средств, используемых для обработки ПДн;
- конфигурация и топология ИСПДн в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- способы физического подключения и логического взаимодействия компонент ИСПДн, способы подключения к сетям связи общего пользования и международного информационного обмена с определением пропускной способности линий связи;
- режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;
- состав используемого комплекса средств защиты ПДн и механизмов идентификации, аутентификации и разграничения прав доступа пользователей ИСПДн на уровне операционных систем, баз данных и прикладного программного обеспечения;

– перечень организационно-распорядительной документации, определяющей порядок обработки и защиты ПДн у Оператора;
– физические меры защиты ПДн, организация пропускного режима.

5.3. Результаты анализа изменений используются для оценки корректности требований по обеспечению безопасности ПДн, обрабатываемых с использованием средств автоматизации и без использования таких средств, и при необходимости их уточнения.

5.4. У Оператора должен вестись учет действий, совершаемых работниками Оператора при обработке ПДн в ИСПДн. Действия с ПДн учитываются в log-файлах ИСПДн и/или в отдельной базе данных ИСПДн.

5.5. Доступ к ПДн осуществляется в соответствии с Регламентом по допуску работников и третьих лиц к обработке ПДн, утвержденным Оператором.

5.6. Лица, допущенные к обработке ПДн, должны быть проинформированы:
– о допуске к обработке ПДн путем ознакомления с Перечнем должностей и третьих лиц, имеющих доступ к ПДн, обрабатываемым у Оператора;
– о категориях, обрабатываемых ПДн путем ознакомления с утвержденным Перечнем обрабатываемых ПДн;
– о правилах осуществления обработки ПДн путем ознакомления под роспись с Положением об обработке ПДн.

5.7. Неавтоматизированная обработка ПДн должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения материальных носителей и установить перечень лиц, допущенных к обработке ПДн. У Оператора должен вестись учет носителей ПДн.

5.8. Фиксация ПДн должна осуществляться на отдельных материальных носителях (отдельных документах). ПДн должны отделяться от иной информации.

5.9. Фиксация на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы, не допускается. В случае если на одном материальном носителе все же зафиксированы ПДн, цели обработки которых несовместимы, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:
– при необходимости использования или распространения определенных ПДн осуществляется выборочное копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется);

– при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным выборочным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

5.10. Правила учета, хранения и уничтожения ПДн при неавтоматизированной обработке описаны в Регламенте по учёту, хранению и уничтожению носителей ПДн, утвержденном Оператором.

5.11. Должен осуществляться мониторинг фактов несанкционированного доступа к ПДн и приниматься соответствующие меры при их обнаружении. Мониторинг осуществляется Администратором безопасности ИСПДн.

5.12. Администратором безопасности ИСПДн должен осуществляться контроль за принимаемыми мерами по обеспечению безопасности ПДн.

5.13. При обработке ПДн Оператор должен иметь возможность и средства для восстановления ПДн, в случае их модификации или уничтожении вследствие несанкционированного доступа к ним. Правила резервного копирования и восстановления ПДн Оператором установлены в Регламенте по резервному копированию ПДн, утвержденному Оператором.

5.14. Оператор определяет перечень помещений, используемых при обработке ПДн. При этом организация режима безопасности, охрана этих помещений должны обеспечивать сохранность носителей ПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

5.15. Пользователи ИСПДн должны обеспечивать сохранность съемных носителей, содержащих ПДн. В случае утраты носителя пользователи должны немедленно сообщить об этом Администратору безопасности ИСПДн.

5.16. Если при работе с ПДн работнику Оператора необходимо покинуть рабочее место, материальные носители ПДн должны быть защищены от неконтролируемого доступа к ним. Для этого материальные носители помещаются в отведенных для хранения места.

5.17. В случае достижения цели обработки ПДн Оператор прекращает обработку ПДн или обеспечивает ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и уничтожает ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого,

выгодоприобретателем или поручителем по которому является субъект ПДн. В случае если ПДн невозможно уничтожить, то они блокируются и уничтожаются в срок, не превышающий шести месяцев.

5.18. Проведение работ по созданию (модернизации) СЗПДн включает следующие стадии:

- предпроектная стадия;
- стадия проектирования;
- стадия реализации СЗПДн;
- стадия ввода в действие СЗПДн.

5.19. На предпроектной стадии проводится определение уровня защищенности ПДн, обрабатываемых в ИСПДн, формируется Модель угроз безопасности ПДн при их обработке в ИСПДн, разрабатывается Техническое задание на СЗПДн.

5.20. Определение уровня защищенности ПДн, обрабатываемых в ИСПДн осуществляется в соответствии с Регламентом по определению уровня защищенности ПДн, обрабатываемых в ИСПДн.

5.21. ИСПДн Оператора указаны в Перечне ИСПДн.

5.22. Уровень защищенности ПДн, обрабатываемых в ИСПДн, оформляется соответствующим актом.

5.23. Модель угроз безопасности ПДн при их обработке в ИСПДн формируется на основании руководящих документов ФСТЭК России и ФСБ России.

5.24. Перечень актуальных угроз формируется для каждой ИСПДн Оператора с учетом условий функционирования ИСПДн и особенностей обработки ПДн.

5.25. По итогам определения уровня защищенности ПДн, обрабатываемых в ИСПДн и результатам определения актуальных угроз безопасности ПДн формируются требования по обеспечению безопасности ПДн, обрабатываемых в ИСПДн. Данные требования оформляются в виде технического задания на СЗПДн.

5.26. Стадия проектирования СЗПДн включает разработку СЗПДн в составе ИСПДн, а именно разработку разделов задания и проекта проведения по созданию (модернизации) СЗПДн в соответствии с требованиями технического задания;

5.27. Стадия реализации СЗПДн включает:

- закупку совокупности используемых в СЗПДн сертифицированных технических, программных и программно-технических средств защиты информации и их установку;

- определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением;
- разработку эксплуатационной документации на СЗПДн и средства защиты информации.

5.28. На стадии ввода в действие СЗПДн осуществляются:

- предварительные испытания средств защиты информации в комплексе с другими техническими и программными средствами;
- устранение несоответствий по итогам предварительных испытаний;
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПД;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

5.29. В процессе функционирования ИСПДн может осуществляться модернизация СЗПДн. В обязательном порядке модернизация проводится в случае, если:

- произошло изменение номенклатуры обрабатываемых ПДн, влекущее за собой изменение уровня защищенности ПДн, обрабатываемых в ИСПДн;
- произошло изменение номенклатуры и/или актуальности угроз безопасности ПДн;
- изменилась структура ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн и т.п.);
- произошло изменение законодательства Российской Федерации в области ПДн, затрагивающее вопросы обеспечения безопасности ПДн при их обработке в ИСПДн.

5.30. При возникновении условий, влияющих на безопасность ПДн (компрометация паролей, нарушение целостности и доступности ПДн и пр.) работник Оператора обязан незамедлительно проинформировать об этом Администратора безопасности ИСПДн.

5.31. Лица, виновные в нарушении требований, предъявляемых законодательством РФ к защите ПДн, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Лист регистрации изменений

Порядковый номер и дата внесении изменений	Наименование документа, фиксирующего изменения	№ замененных (исправленных) листов	Подпись лица, внесшего изменения