ДЕПАРТАМЕНТ СОЦИАЛЬНОГО РАЗВИТИЯ
ХАНТЫ – МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА – ЮГРЫ
(ДЕПСОЦРАЗВИТИЯ ЮГРЫ)
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ХАНТЫ – МАНСИЙСКОГО
АВТОНОМНОГО ОКРУГА – ЮГРЫ
«НЕФТЕЮГАНСКИЙ РАЙОННЫЙ КОМПЛЕКСНЫЙ ЦЕНТР
СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ»
(БУ «НЕФТЕЮГАНСКИЙ РАЙОННЫЙ КОМПЛЕКСНЫЙ ЦЕНТР
СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ»)

ПРИКАЗ

«21» 08 2020г. №335
гп. Пойковский

Об утверждении организационно – распорядительной документации в отношении обработки персональных данных

Во исполнение требований Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 года №152-ФЗ «О персональных данных» и принятых в соответствии с ними нормативно-правовых актов, а также в целях обеспечения защиты персональных данных и другой защищаемой информации, обрабатываемой в информационной сети БУ «Нефтеюганский районный комплексный центр социального обслуживания населения»

ПРИКАЗЫВАЮ:

1. Утвердить:
1.1. Действие приказа от 12 марта 2018 года № 103 «Об утверждении организационно – распорядительной документации в отношении обработки персональных данных» считать не действительным.
1.2. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение 1);
1.3. Инструкцию по регистрации событий безопасности (Приложение 2);
1.4. Политику в отношении обработки персональных данных в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» (Приложение 3);

1.5. Функции и задачи работников, эксплуатирующих информационную систему обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» (Приложение 4);

1.6. Функции и задачи должностного лица, ответственного за организацию обработки персональных данных БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» (Приложение 5);

1.7. Функции и задачи должностного лица, ответственного за руководство работами по защите информации в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» (Приложение 6).

2. Руководителям структурных подразделений ознакомить под роспись сотрудников отделений с утвержденными организационно-распорядительными документами.

3. Документоведу ознакомить под роспись заинтересованных лиц.

4. Контроль за исполнением приказа оставляю за собой.

Директор Е.М. Елизарьева

Приложение 1
к приказу от 21.08.2020 № 335

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных (далее - ПДн) в Учреждении требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Правила), разработаны в соответствии с Федеральным законом от 27.07.2006№ 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006№ 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных, а также определяют основания, порядок и методы проведения внутреннего контроля соответствия обработки ПДн требованиям законодательства Российской Федерации.

2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных к требованиям защиты персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям к защите ПДн в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» организовывается проведение ежегодных проверок.

2.2. Проверки проводятся ответственным за организацию обработки ПДн совместно с ответственным за обеспечение безопасности ПДн и другой защищаемой информации, обрабатываемой в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» и ответственными за эксплуатацию информационных систем персональных данных БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» (далее - ИСПДн БУ «Нефтеюганский районный комплексный центр социального обслуживания населения»).

2.3. Плановые проверки условий обработки ПДн проводятся на основании утвержденного руководителем БУ «Нефтеюганский районный комплексный

центр социального обслуживания населения» ежегодного плана внутренних проверок режима защиты ПДн (плановые проверки).

2.4. Внеплановые проверки проводятся на основании поступившей информации о нарушениях правил обработки ПДн, по инициативе ответственного за организацию обработки ПДн, либо ответственного за обеспечение безопасности ПДн и другой защищаемой информации, обрабатываемой в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения». Проведение внеплановой проверки организуется в течение 10 (десяти) рабочих дней со дня поступления информации о нарушениях правил обработки ПДн.

2.5. В проведении проверки условий обработки ПДн не могут участвовать сотрудники БУ «Нефтеюганский районный комплексный центр социального обслуживания населения», прямо или косвенно заинтересованных в ее результате.

2.6. Проверки условий обработки ПДн осуществляются непосредственно на месте обработки ПДн путем опроса либо, при необходимости, путем осмотра служебных мест сотрудников БУ «Нефтеюганский районный комплексный центр социального обслуживания населения», участвующих в процессе обработки ПДн.

2.7. При проведении проверки должны быть полностью, объективно и всесторонне, установлены:

соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям БУ «Нефтеюганский районный комплексный центр социального обслуживания населения»;

соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;

достаточность (избыточность) ПДн для целей обработки ПДн, заявленных при сборе ПДн;

отсутствие (наличие) объединения, созданных для несовместимых между собой целей, баз данных ИСПДн;

порядок и условия применения организационных и технических мер по обеспечению безопасности ПДн при их обработке, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн;

порядок и условия соблюдения парольной защиты; порядок и условия соблюдения антивирусной защиты; порядок и условия обеспечения резервного копирования; эффективность принимаемых мер по обеспечению безопасности ПДн до их ввода в ИСПДн;

условия соблюдения режима защиты при подключении к информационно-телекоммуникационным сетям;

порядок и условия обновления программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн;

порядок и условия применения средств защиты информации; соблюдение учета носителей ПДн; соблюдение правил доступа к ПДн;

соблюдение порядка доступа в помещения, в которых ведется обработка ПДн;

наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;

мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

осуществление мероприятий по обеспечению целостности ПДн.

2.8. Ответственный за организацию обработки ПДн и ответственный за обеспечение безопасности ПДн и другой защищаемой информации, обрабатываемой в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения», а также ответственные за эксплуатацию ИСПДн Департамента в ходе проверки имеют право:

запрашивать у сотрудников информацию, необходимую для реализации своих полномочий;

требовать от уполномоченных на обработку ПДн сотрудников уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;

принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;

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

вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПДн.

2.9. Проверка условий обработки ПДн должна быть завершена не позднее чем через тридцать календарных дней со дня принятия решения о ее проведении.

2.10. По результатам проведенной проверки условий обработки ПДн ответственный за организацию обработки ПДн предоставляет руководителю БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» письменное заключение с указанием мер, необходимых для устранения выявленных нарушений.

Приложение 6
к приказу от _____№ ___

ИНСТРУКЦИЯ
по регистрации событий безопасности

1. Общие положения

Настоящая инструкция разработана в соответствии с п. 8.5 приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», п. 20.5 приказа ФСТЭК России от № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.1. Событие безопасности (информационной) - это идентифицированное возникновение состояния информационной системы персональных данных (сегмента, компонента информационной системы персональных данных), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

1.2. Отслеживание событий (проверку), происходивших на автоматизированных рабочих местах (далее - АРМ), осуществляет ответственный за обеспечение безопасности персональных данных (далее - ПДн) в информационных системах персональных данных (далее -администратор информационной безопасности).

1.3. Общими задачами проверки являются:

контролирование состояния защищенности системы;

выявление причин произошедших изменений;

определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД; установление времени изменений.

2. Определение событий безопасности, подлежащих регистрации, их состава, содержания и сроков хранения

2.1. События, происходящие на АРМ, входящих в состав ИСПДн, регистрируются в журналах, приведенных в п. 3.1. настоящей инструкции.

2.2. Каждому событию соответствует отдельная запись в журнале, содержащая подробную информацию для анализа события.

2.3. В информационных системах персональных данных как минимум подлежат регистрации следующие события:

вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (останова) операционной системы;

подключение машинных носителей информации и вывод информации на носители информации;

запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа; попытки удаленного доступа.

2.4. При регистрации входа (выхода) субъектов доступа в ИСПДн и загрузки (останова) операционной системы состав и содержание информации, как минимум, включают дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2.5. При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей, как минимум, включают дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

2.6. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей, как минимум, включают дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

2.7. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей, как минимум, включают дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

2.8. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации, как минимум, включают дату и время попытки доступа к защищаемому

объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

2.9. При регистрации попыток удаленного доступа к информационным системам персональных данных состав и содержание информации, как минимум, включают дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

2.10. Срок хранения событий безопасности составляет 3 месяца для оперативного доступа, 12 месяцев - архивного хранения.

2.11. События безопасности подлежат защите, реализуемой организационным и техническими мерами, и соответствующим настройкам системы защиты информации на ограничение доступа пользователей к параметрам настройки средств защиты информации.

3. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

3.1. События безопасности регистрируются в:
штатных журналах операционной системы Windows;
журналах событий средств защиты информации.

3.2. Администратор информационной безопасности производит проверку электронных журналов не реже одного раза в неделю с внесением соответствующей информации в «Журнале учета внутренних проверок режима защиты персональных данных».

3.3. В случае сбоя при регистрации событий безопасности осуществляется предупреждение (сигнализация, индикация) администратора информационной безопасности о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности.

3.4. При обнаружении сбоя при регистрации событий безопасности администратор информационной безопасности обязан реагировать путем изменения параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

3.5. Администратор информационной безопасности совместно с ответственным за организацию обработки ПДн принимают решение об определении события информационной безопасности к относящимся или не относящимся к инцидентам информационной безопасности. Инциденты информационной безопасности могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами. Их последствиями могут быть такие события, как несанкционированные раскрытие или изменение ПДн, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» или их хищение.

3.6. В случае обнаружения инцидента информационной безопасности администратор информационной безопасности руководствуется Инструкцией по работе с инцидентами информационной безопасности.

Приложение 3

к приказу от _____№ ___

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В БУ «Нефтеюганский районный комплексный центр социального обслуживания населения»

Содержание:

1. Термины и определения

1.1. Персональные данные (далее - ПДн) - любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу.

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

1.3. 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 ПДн.

1.4. Автоматизированная обработка персональных данных - обработка ПДн с помощью средств вычислительной техники.

1.5. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.6. Использование персональных данных - действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом, затрагивающих права и свободы субъекта ПДн или других лиц.

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

1.8. Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

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

1.11. Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства Учреждению иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Назначение и область применения

Настоящая Политика в отношении обработки персональных данных в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» (далее - Политика) разработана в соответствии со статьей 18.1 Федерального закона от № 152-ФЗ «О персональных данных» (далее - Закон № 152-ФЗ) и действует в отношении всех персональных данных, которые Департамент социального развития Ханты-Мансийского автономного округа - Югры (далее - Оператор) может получить от субъектов персональных данных.

2.1. Политика распространяется на персональные данные, полученные как до, так и после её утверждения приказом Оператора.

2.2. Действие настоящей Политики распространяется на все процессы обработки персональных данных Оператором, как с использованием средств автоматизации, так и без использования таких средств, на всех работников Оператора, участвующих в таких процессах, а также на информационные системы БУ «Нефтеюганский районный комплексный центр социального обслуживания населения», используемые в процессах обработки персональных данных.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных осуществляется Оператором на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей. Оператором не допускается обработка персональных данных, несовместимая с целями сбора персональных данных и объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.2. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых Оператором персональных данных соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается.

3.3. При обработке персональных данных Оператором обеспечивается точность персональных данных, их достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных. Оператором принимаются необходимые меры (обеспечивается их принятие) по удалению или уточнению неполных или неточных персональных данных.

3.4. При определении состава обрабатываемых персональных данных субъектов персональных данных Оператор руководствуется минимально необходимым составом персональных данных для достижения целей получения персональных данных.

3.5. Хранение персональных данных Оператором осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Условия обработки персональных данных

4.1. Обработка персональных данных осуществляется в соответствии с целями, заранее определенными и заявленными при сборе персональных данных, а также полномочиями Оператора, определенными действующим законодательством Российской Федерации и договорными отношениями с Оператором.

4.2. Получение и обработка персональных данных в случаях, предусмотренных законом № 152-ФЗ, осуществляется Оператором только с письменного согласия субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью.

4.3. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой

позволяющей подтвердить факт его получения форме, если иное не установлено законом № 152-ФЗ. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Оператором.

4.4. Оператор вправе обрабатывать персональные данные без согласия субъекта персональных данных (или при отзыве субъектом персональных данных согласия на обработку персональных данных) при наличии оснований, указанных в законе № 152-ФЗ.

4.5. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, Оператором не осуществляется.

4.6. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные) и сведения о состоянии здоровья, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных или иных оснований, предусмотренных федеральным законодательством.

4.7. Персональные данные субъекта могут быть получены Оператором от лица, не являющегося субъектом персональных данных, при условии предоставления Оператору подтверждения наличия оснований, указанных в законе № 152-ФЗ или иных оснований, предусмотренных федеральным законодательством.

4.8. Право доступа к персональным данным субъектов персональных данных на бумажных и электронных носителях имеют работники Оператора в соответствии с их должностными обязанностями.

4.9. Оператором не осуществляется трансграничная передача персональных данных и не принимаются решения, основанные исключительно на автоматизированной обработке персональных данных субъекта.

5. Цели обработки персональных данных

5.1. В соответствии с принципами и условиями обработки персональных данных, Оператором определены следующие цели обработки ПДн:

выполнение обязательств, предусмотренных служебным контрактом;

выполнение требований Трудового кодекса Российской Федерации других нормативных актов Российской Федерации (в том числе предоставление персональных данных в Пенсионный; фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования);

принятие решений и выполнение обязательств по обращениям граждан Российской Федерации в соответствии с законодательством Российской Федерации;

оказание государственных услуг гражданам.

6. Особенности обработки персональных данных и их передача третьим лицам

6.1. Обработка персональных данных Оператором осуществляется как с использованием средств автоматизации, так и без использования таких средств.

При обработке персональных данных Оператор осуществляет следующие действия с персональными данными: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

6.2. Передача персональных данных субъектов персональных данных третьим лицам осуществляется Оператором в соответствии с требованиями действующего законодательства.

6.3. Оператор вправе поручить обработку персональных данных третьей стороне с согласия субъекта персональных данных и в иных случаях, предусмотренных действующим законодательством Российской Федерации, на основании заключаемого с этой стороной соглашения, (далее - поручение). Третья сторона, осуществляющая обработку персональных данных по поручению Оператора, обязана соблюдать принципы и правила обработки персональных данных, предусмотренные законом № 152-ФЗ, обеспечивая конфиденциальность и безопасность персональных данных при их обработке.

7. Права субъектов персональных данных

7.1. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

подтверждение факта обработки персональных данных Оператором; правовые основания и цели обработки персональных данных, применяемые Оператором способы обработки ПДн;

наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), 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;

порядок осуществления субъектом ПДн прав, предусмотренных законом № 152-ФЗ;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу; иные сведения, предусмотренные законом № 152-ФЗ.

8. Обеспечение безопасности персональных данных

8.1. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. К данным мерам в частности

относится: назначение лица, ответственного за организацию обработки персональных данных;
осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
ознакомление работников Оператора с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных, требованиями к защите персональных данных;
издание локальных актов по вопросам обработки персональных данных и локальных актов, устанавливающих процедуры, направленные на предотвращение и выявления нарушений законодательства Российской Федерации;
определение угроз безопасности персональных данных и необходимого уровня защищённости персональных данных, при их обработке в ИСПДн;
применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн;
использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;
осуществление оценки эффективности применяемых мер по обеспечению безопасности персональных данных.

Приложение 4
к приказу от _____№ ___

Типовые функции и задачи работников, эксплуатирующих информационную систему обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения»

1.Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность работников, эксплуатирующих информационную систему БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» (далее - Пользователь) информационных систем обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные (далее - ИС) БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» (далее -Учреждение).

1.2. Пользователем ИС является работник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС, в соответствии со Списком лиц, допущенных к самостоятельной работе в ИС.

1.3. Пользователь должен принимать все необходимые меры по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных (далее - конфиденциальная информация (КИ)) и контролю за соблюдением прав доступа к ней.

1.4. Положения настоящего документа обязательны для исполнения всеми пользователями.

Все пользователи должны быть ознакомлены под роспись с настоящим документом и предупреждены об индивидуальной ответственности за его нарушения.

1.5. Основными задачами при обработке информации в ИС являются:
обеспечение исполнения требований нормативных правовых актов, руководящих документов, регламентирующих защиту информации в Российской Федерации в процессе создания, хранения и передачи документов, содержащих конфиденциальную информацию в ИС Учреждения;

обеспечение в ИС необходимого уровня безопасности обработки, хранения и передачи КИ;
обеспечение необходимого уровня безопасности носителей КИ;
обеспечение безопасности конфиденциальной информации при ее копировании, размножении;
резервное копирование, восстановление информации.

2. Основные положения

2.1. При первичном допуске к работе в ИС пользователь изучает требования настоящего документа, разрешительную систему доступа к ИС, технологический процесс обработки информации в ИС, руководящие, нормативно-методические и организационно-распорядительные документы по вопросам обеспечения безопасности обрабатываемой информации.

2.2. Каждый пользователь ИС, имеющий в рамках своих обязанностей доступ к аппаратным средствам, программному обеспечению и данным ИС, несет персональную ответственность за свои действия и обязан:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС, в том числе положения настоящего документа;

знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции;

располагать основные технические средства и системы (далее -ОТСС) в соответствии с техническим паспортом;

хранить в тайне свой пароль (пароли), парольную защиту организовывать в соответствии с инструкцией по организации парольной защиты;

выполнять требования «Инструкции по организации антивирусной защиты»;

немедленно вызывать администратора безопасности и ставить в известность руководителя подразделения при подозрении компрометации личных ключей и паролей или при обнаружении фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к основным техническим средствам и системам (далее - ОТСС) ИС;

в случае появления у пользователя сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах или попытках НСД к информации, обрабатываемой в ИС, пользователь должен немедленно сообщить об этом администратору безопасности;

немедленно сообщать администратору информационной безопасности об обнаруженных фактах нарушения информационной безопасности кем-либо;

сообщать администратору информационной безопасности об отклонениях в нормальной работе установленных на рабочей станции средств защиты информации;

при работе в ИС выполнять только служебные задания;

при отсутствии необходимости работы выключить (блокировать) компьютер;

при работе в ИС использовать только учтенные съемные носители, при обоснованной необходимости использования неучтённых носителей согласовывать использование с администратором информационной безопасности. После того как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.) информация незамедлительно удаляется с носителей;

осуществлять установленным порядком уничтожение информации (сочетанием клавиш Shift+Del), содержащей сведения конфиденциального характера, с машинных (съемных) носителей информации

немедленно выполнять предписания администратора безопасности в части обеспечения безопасности информации;

экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;

соблюдать установленный режим разграничения доступа к информационным ресурсам;

не разглашать известную им информацию, составляющую конфиденциальную информацию лицам, не имеющим допуска к этой информации;

все изменения конфигурации технических и программных средств ИС, ремонт, модификация и техническое обслуживание технических средств и систем, входящих в состав ИС производить только на основании «Инструкции пользователю по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств».

2.3. Пользователю запрещается:

самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств, устанавливать или удалять установленные техническим специалистом (администратором информационной безопасности) сетевые программы на компьютерах, вскрывать компьютеры, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование, вносить какие - либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства без согласования с администратором безопасности;

привлекать посторонних лиц для производства ремонта ОТСС без письменной заявки и согласования с администратором информационной безопасности;

запускать любые системные или прикладные программы, не входящие в состав программного обеспечения;

работать с неучтенными машинными (съемными) носителями информации; отключать (блокировать) средства защиты информации; производить какие-либо изменения в размещении технических средств;

обрабатывать на средствах вычислительной техники (далее - СВТ) входящих в состав ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам;

сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ИС;

хранить на учтенных носителях программы и данные, не относящиеся к рабочей информации;

выполнять работы с документами ограниченного распространения на дому, выносить их за пределы контролируемой зоны;

передавать свои учтённые носители кому-либо;

вводить в ОТСС персональные данные под диктовку или с микрофона;

осуществлять попытки несанкционированного доступа к ресурсам ИСПДн, проводить или участвовать в сетевых атаках и сетевом взломе;

производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и серверов;

закрывать доступ к информации паролями без согласования с администратором информационной безопасности;

оставлять без личного присмотра на рабочем месте или где бы то ни было персональное устройство идентификации, машинные (съемные) носители и распечатки, содержащие защищаемую информацию;

2.4. Пользователь обязан обеспечить:

сохранность оборудования и физической целостности системных блоков компьютеров;

блокирование своей учетной записи в случае кратковременного оставления АРМ (нажатием клавиш Windows+L);

обязательное выключение компьютера после завершения работы.

3. Права пользователя:

участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС, если данное нарушение произошло под его идентификационными данными;

своевременно получать доступ к информационным ресурсам ИС, необходимым ему для выполнения своих должностных обязанностей;

требовать от администратора информационной безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

Ответственность:

3.1. пользователь несет персональную ответственность за соблюдение установленных требований во время работы. Пользователи, виновные в нарушении законодательства Российской Федерации о защите прав собственности и охраняемых по Закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно распорядительными документами;

3.2. пользователь отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники;

3.3. нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей или ИСПДн в целом, может повлечь ответственность в соответствии с действующим законодательством.

4. Работа с файлами документов, внесение корректировок, уничтожение, хранение документов

№ п.п	Этап	Описание этапа
1 . Подготовка к обработке информации		
1	Получение допуска к работе	Допуск работников Учреждения к ИС осуществляется в соответствии с Списком лиц, допущенных к самостоятельной работе на ИС и разрешительной системе допуска к информационным ресурсам и техническим средствам. Для работы в ИС каждый пользователь должен получить соответствующий допуск. Права по доступу к информационным ресурсам
2	Получение исходной информации для обработки в системе	Исходная информация, обработка которой осуществляется в системе, может находиться на учтённых сменных носителях информации (съемных жестких дисках, дискетах, компакт-дисках, бумажных носителях)
3	Вход пользователя в систему	Авторизация пользователя осуществляется средствами защиты информации по имени и с использованием его персонального пароля длиной не менее 6 символов
2. Обработка информации		
1	Регистрация времени начала работы	Осуществляется средствами защиты информации
2	Ввод обрабатываемых исходных данных в систему	Ввод в систему обрабатываемой информации производится вручную с клавиатуры или путем считывания в электронном виде с дискет или компакт-дисков.
3	Обработка текстовой информации	Пользователь обязан принять меры по исключению возможности просмотра обрабатываемой информации с экрана монитора и с бумажных носителей (в том числе распечатываемых материалов) лицами, не допущенными к обрабатываемой информации.
4	Временное хранение обрабатываемой информации между сеансами работы пользователя в системе	Хранение обрабатываемой информации, между сеансами работы в системе, пользователь осуществляет в каталогах на жестком диске ПЭВМ, выделенных в системе для соответствующих видов обрабатываемой информации. Контроль доступа к ним осуществляется соответствующими средствами защиты информации
3. Сохранение результатов обработки информации		

1	Распечатка документов	Распечатка документов (данных) производится на принтере, входящем в состав ОТСС объекта, средствами защиты информации может осуществляться учет распечатанных документов.
2	Сохранение окончательных результатов работы	Готовые данные в электронном виде содержатся на жёстком диске ОТСС ИС, регистрация и контроль доступа к ним осуществляется средствами защиты информации.
3	Передача носителей информации и распечатанных документов	В соответствии с требованиями организационно-распорядительных документов Аппарата Губернатора и Правительства автономного округа
4	Очистка остаточной (удаленной) информации	Гарантированная очистка удаляемой с накопителей информации (без возможности ее восстановления) осуществляется средствами защиты информации
5	Регистрация времени работы и действий пользователя в	Осуществляется средствами защиты информации
6	Завершение работы	После окончания работы с ИС, сотрудник обязан на своем рабочем месте завершить работу всех программ, входящих в состав специализированного программного обеспечения и выключить компьютер (перегрузить). В случаи необходимости оставить свое рабочее место на непродолжительное время пользователь обязан его заблокировать (дальнейшая работа может быть продолжена пользователем только после ввода его логина и пароля). После окончания рабочего дня необходимо закрыть окна и форточки, выключать электроприборы, запереть дверь и включить охранную сигнализацию, при наличии таковой

5. Подготовка, отправка, размножение, копирование, учет, распечатка необходимого числа экземпляров подготовленных документов, содержащих информацию ограниченного доступа.

Печать производится на принтере, входящем в состав ИС.
Размножение (копирование) документов, содержащих информацию ограниченного доступа, осуществляется только на МФУ, входящих в состав аттестованного СВТ или на аттестованном средстве изготовления и размножения документов (копир) Учреждения.

Подготовка, учет, отправка, документов содержащих информацию ограниченного доступа осуществляется в соответствии с требованиями раздела XI «Порядок обращения с конфиденциальной информацией» постановления Губернатора Ханты-Мансийского

автономного округа -Югры от 30 декабря 2012 года № 176 «Об Инструкции по делопроизводству в государственных органах Ханты-Мансийского автономного округа - Югры и исполнительных органах государственной власти Ханты-Мансийского автономного округа - Югры» (с изменениями, внесенными постановлением Губернатора автономного округа № 57).

Приложение 5
к приказу_____ от___

Типовые функции и задачи должностного лица, ответственного за организацию обработки персональных данных в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения»

1. Общие положения

1.1. Инструкция лица, ответственного за организацию обработки персональных данных в исполнительном органе государственной власти Ханты-Мансийского автономного округа - Югры (далее - Инструкция), разработана в соответствии с требованиями постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных па обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Инструкция закрепляет обязанности, права и ответственность лица, ответственного за организацию обработки персональных данных в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения» (далее - Учреждение).

1.3. Лицо, ответственного за организацию обработки персональных данных в органе назначается распорядительным документом Учреждения.

1.4. Лицо, ответственное за организацию обработки персональных данных, в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами, настоящей Инструкцией, а также иными локальными нормативными актами организации, регламентирующими вопросы обработки персональных данных Учреждения.

1.5. Лицо, ответственное за организацию обработки персональных данных в Аппарате Губернатора Югры определяет лиц, ответственных за контроль выполнения требований по обработке персональных данных, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами в структурных подразделениях Учреждения.

1.6. Перечень лиц, ответственных за контроль выполнения требований по обработке персональных данных в структурных подразделениях Учреждения (по должностям) утверждает руководитель Учреждения.

2. Должностные обязанности лица, ответственного за организацию обработки персональных данных в Учреждение

2.1. Лицо, ответственное за организацию обработки персональных данных в Учреждение обязан знать:

перечень персональных данных (далее - ПДн) обрабатываемых в Учреждение;

перечень информационных систем персональных данных Учреждения (далее - ИСПДн);

перечень должностей работников Учреждение, замещение которых предусматривает осуществление обработки персональных данных, либо

осуществление доступа к персональным данным;

условия и технологический процесс обработки персональных данных в Учреждении;

законодательство Российской Федерации о персональных данных, следить за его изменениями, своевременно и точно отражать изменения в локальных организационных актах по управлению средствами защиты информации в ИСПДн и правилам обработки ПДн.

2.2. Лицо, ответственное за организацию обработки персональных данных в Учреждении обязано:

предоставлять на утверждение Руководителю Учреждения перечень должностей работников Учреждения, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным и изменения к нему;

участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей;

контролировать выполнение мероприятий защите информации в ИСПДн;

вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных в следствии неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

проводить занятия и инструктажи с работниками Учреждения о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности ПДн;

контролировать соблюдение работниками Учреждения локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными, машинными носителями информации;

осуществлять внутренний контроль за соблюдением работниками Учреждения требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных;

представлять интересы Учреждения при проверках надзорных органов в сфере обработки персональных данных;

выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

3. Должностные обязанности лиц, ответственных за контроль выполнения требований по обработке персональных данных в структурных подразделениях Учреждения

3.1. Лицо, ответственное за контроль выполнения требований по обработке ПДн в структурных подразделениях Учреждения организует в структурных подразделениях Учреждения обработку ПДн в соответствии с требованиями предусмотренными федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Лицо, ответственное за контроль выполнение требований по обработке ПДн в структурных подразделениях Учреждения выполняет указания и распоряжения лица, ответственного за организацию обработки ПДн в Учреждении.

3.2. Лицо, ответственное за контроль выполнения требований по обработке персональных предусмотренных в структурных подразделениях Учреждения обязан знать:

перечень ПДн обрабатываемых в структурном подразделении Учреждения;

перечень и состав ИСПДн структурного подразделения Учреждения;

перечень должностей работников структурного подразделения Учреждения, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным;

перечень лиц, допущенных к самостоятельной обработки ПДн в ИСПДн;

условия и технологический процесс обработки ПДн в структурном подразделении Учреждения;

законодательство Российской Федерации о персональных данных, следить за его изменениями, своевременно и точно отражать изменения в локальных организационных актах по управлению средствами защиты информации в ИСПДн и правилам обработки ПДн.

3.4. Лицо, ответственное за контроль выполнения требований по обработке ПДн в структурных подразделениях Учреждения обязано:

своевременно представляет перечень должностей работников Учреждения, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным и изменения к нему лицу, ответственному за организацию обработки ПДн в Учреждении;

осуществлять учет лиц, допущенных к работе с персональными данными в журнале учета лиц, допущенных к работе с персональными данными в ИСПДн структурного подразделения Учреждения»;

доводить до сведения работников структурного подразделения Учреждения положения законодательства Российской Федерации в области ПДн, локальных актов по вопросам обработки персональных данных, требований к защите ПДн;

организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов;

осуществлять фиксацию фактов обращений и запросов субъектов персональных данных или их представителей в журнале учета обращений граждан (субъектов ПДн) о выполнении их законных прав при обработке персональных данных в Учреждении;

принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных;

осуществлять взаимодействие по обеспечению безопасности персональных данных с администратором информационной безопасности;

участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей;

осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения;

блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки;

своевременно реагировать на попытки несанкционированного доступа к информации.

контролировать осуществление мероприятий по установке и настройке средств защиты информации;

вносить свои предложения по совершенствованию мер защиты ПДн в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости ПДн в следствии неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования,

предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

проводить занятия и инструктажи с работниками Учреждения о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности ПДн;

контролировать соблюдение работниками структурного подразделения Учреждения локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными, машинными носителями информации;

осуществлять внутренний контроль за соблюдением работниками структурного подразделения Учреждения требований законодательства Российской Федерации в области персональных данных;

выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

4. Действия при обнаружении попыток несанкционированного доступа

4.1. К попыткам несанкционированного доступа относятся:

сеансы работы с ПДн незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа лицо, выявившее факт несанкционированного доступа (пользователи, ответственный за организацию обработки ПДн, лицо, ответственное за выполнение требований по обработке ПДн в структурных подразделениях Учреждения, администратор

информационной безопасности) обязаны:

законными способами прекратить несанкционированный доступ к ПДн;

известить администратора информационной безопасности ИСПДн о факте несанкционированного доступа;

известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

известить руководство Учреждения.

4.3. Лицо, ответственное за руководство работами по защите информации в Учреждение, организует разбирательство по факту несанкционированного доступа;

4.4. По результатам разбирательства лицо, ответственное за организацию обработки ПДн докладывает заместителю руководителя лицу, ответственному за руководство работами по защите информации в Учреждение служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях.

5. Права

5.1. Ответственный за организацию обработки ПДн в Учреждение и лица, ответственные за контроль выполнения требований по обработке персональных данных в структурных подразделениях Учреждения имеют право:

требовать от работников выполнения федерального закона «О персональных данных» и принятых в соответствии с ним нормативными правовыми актами, а также локальных нормативно-правовых актов в части работы с персональными данными;

блокировать доступ к ПДн любых пользователей, если это необходимо для предотвращения нарушения режима защиты ПДн; проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных;

привлекать к реализации мер, направленных на выполнение требований законодательства о персональных данных, иных работников Учреждения с возложением на них соответствующих обязанностей и закреплением ответственности;

иметь доступ к информации, касающейся обработки персональных данных в соответствующем структурном подразделении Учреждения и включающей:

цели обработки персональных данных;

категории обрабатываемых персональных данных;

категории субъектов, персональные данные которых обрабатываются;

правовые основания обработки персональных данных;

перечень действий с персональными данными, общее описание используемых в центральном аппарате Роскомнадзора способов обработки персональных данных;

дату начала обработки персональных данных;

срок или условия прекращения обработки персональных данных;

сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

6. Ответственность

6.1. Ответственный за организацию обработки персональных данных в Учреждение и лица, ответственные за контроль выполнения требований по обработке персональных данных в структурных подразделениях Учреждения несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых ими работ по обработке и обеспечению безопасности персональных данных.

6.2. Ответственный за организацию обработки персональных данных в Учреждение и лица, ответственные за контроль выполнения требований по обработке персональных данных в структурных подразделениях Учреждения при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

6.3. Пользователи несут персональную ответственность за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

Приложение 6
к приказу от_____№___

Типовые функции и задачи должностного лица, ответственного за руководство работами по защите информации в БУ «Нефтеюганский районный комплексный центр социального обслуживания населения»

Лицо, ответственное за руководство работами по защите информации в исполнительном Учреждение Ханты-Мансийского автономного округа - Югры выполняет следующие основные функции:

руководство и координация деятельности по обеспечению безопасности информации в соответствии с требованиями законодательством Российской Федерации, нормативных правовых актов Президента и Правительства Российской Федерации, руководящих и методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и ФСБ России;

контроль выполнение работ по информационной безопасности в Учреждение автономного округа;

принимает решение о возможности распространения (передачи) персональных данных и иной конфиденциальной информации;

согласовывает назначение лица, ответственного за организацию обработки персональных данных в Учреждение;

согласовывает назначение лиц, ответственных за контроль выполнения требований по обработке персональных данных в структурных подразделениях Учреждения;

согласовывает назначение администратора информационной безопасности информационных систем Учреждения;

координирует вопросы обучения, повышение квалификации в области обеспечения информационной безопасности в учебных заведениях программы, которых, согласованы ФСТЭК России;

представляет на утверждение руководителю Учреждения перечень лиц, доступ которых к конфиденциальной информации, обрабатываемой в ИС, необходим для выполнения служебных обязанностей;

осуществляет контроль по поддержанию функционирования системы защиты информации в Учреждение;

осуществляет контроль соответствия реального состава пользователей матрице доступа;

осуществляет контроль лиц, допущенных к работе с конфиденциальной информацией в ИС (СВТ);

осуществляет согласование документов, определяющих построение, внедрение, модернизацию системы защиты информации в ИС Учреждения;

осуществляет контроль за уровнем безопасности информации в Учреждение;

инициирует и организовывает проведение служебных проверок по фактам несоблюдения условий, которые могут привести к нарушению конфиденциальности информации или другим нарушениям, приводящим к снижению уровня защищенности информации;

осуществляет координацию и руководство работой ПДТК по ЗИ.