Приложение 3 к приказу № 39
от « 03 » апреля 2017 г.

Положение
об организации и проведении работ по обеспечению безопасности персональных данных и другой защищаемой информации, обрабатываемой в информационных системах закрытого сегмента корпоративной сети в автономном учреждении Ханты-Мансийского автономного округа – Югры «Социально - оздоровительный центр «Сыновья»

1. Общие положения

1.1. Настоящее Положение (далее – Положение) определяет основные требования к порядку создания системы защиты персональных данных (далее – СЗ ПДн), разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Положение имеет своей целью определение комплекса мероприятий по обеспечению безопасности персональных данных.

1.3. Положение вступает в силу с момента его утверждения приказом директора автономного учреждения Ханты-Мансийского автономного округа – Югры «Социально - оздоровительный центр «Сыновья» (далее – Учреждение) и действует бессрочно, до замены его новым Положением.

2. В настоящем Положении используются следующие термины:

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

2.2. **Безопасность персональных данных** - состояние защищенности ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в информационных системах ПДн.

2.3. **Блокирование персональных данных** - временное прекращение обработки ПДн.

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

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

2.6. **Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

2.7**. Контролируемая зона** - территория, в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

2.8. **Обработка персональных данных** - любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение ПДн.

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

2.10. **Использование персональных данных** - действия 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.

2.11. **Пользователь информационной системы персональных данных** - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

2.12. **Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

2.13. **Угрозы безопасности персональных данных** - совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных.

2.14. **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.

2.15. **Целостность информации** - способность средства вычислительной техники или информационной системы обеспечивать

неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Требования по обработке персональных данных

3.1. В целях обеспечения прав и свобод человека и гражданина при обработке персональных данных обязаны соблюдаться следующие требования:

- обработка ПДн субъектов ПДн должна осуществляться с соблюдением требований Федерального закона 152-ФЗ «О защите персональных данных», а также требований постановления Правительства от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации» и иных нормативных правовых актов;
- при определении объёма и содержания обрабатываемых ПДн субъектов ПДн необходимо руководствоваться Конституцией Российской Федерации и иными Федеральными законами;
- ПДн не могут быть использованы в целях причинения имущественного или морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации;
- субъекты ПДн, или их законные представители имеют право ознакомиться с документами, устанавливающими порядок обработки ПДн субъектов.

3.2. Получение персональных данных:

- ПДн следует получать у самого субъекта ПДн. Если ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлён об этом заранее и от него должно быть получено письменное согласие. Учреждение обязано сообщить субъекту ПДн о целях обработки ПДн, о правовом основании, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа субъекта ПДн дать письменное согласие на их получение;
- запрещается получать и обрабатывать ПДн субъекта о его политических, религиозных и иных убеждениях и частной жизни;
- запрещается получать и обрабатывать ПДн субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами;
- запрещается запрашивать информацию о состоянии здоровья субъекта ПДн, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

3.3. При передаче персональных данных субъекта оператор обязан соблюдать следующие требования:

- не сообщать ПДн субъектов ПДн третьей стороне без согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Положением или Федеральными законами;

- предупредить лиц, получающих ПДн субъекта ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн субъектов ПДн, обязаны соблюдать режим конфиденциальности;

- не сообщать ПДн субъекта в коммерческих целях без его письменного согласия;

3.4. К числу массовых потребителей персональных данных вне Учреждения относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, и муниципальных органов управления. Контрольно-надзорные органы имеют доступ к информации только в сфере своей компетенции.

3.5. Организации, в которые субъект может осуществлять перечисления денежных средств могут получить доступ к ПДн субъекта только в случае его письменного разрешения.

3.6. Все меры конфиденциальности при сборе, обработке и хранении ПДн субъекта распространяются как на бумажные, так и на электронные носители информации.

3.7. Все сотрудники, имеющие доступ к персональным данным субъектов, обязаны подписать обязательство о неразглашении информации, обрабатываемой в информационных системах персональных данных Учреждения.

4. Принципы организации защиты персональных данных

4.1. Для обеспечения внутренней защиты персональных данных следует руководствоваться следующими принципами:

- законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

- системность: обработка ПДн в Учреждении осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

- комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Учреждения (далее - ИС) и других имеющихся в Учреждении систем и средств защиты;

- непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Учреждении с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного опыта в сфере защиты информации;

- персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на должностных лиц Учреждения в пределах их обязанностей, связанных с обработкой и защитой ПДн;

- минимизация прав доступа: доступ к ПДн предоставляется должностным лицам только в объеме, необходимом для выполнения их должностных обязанностей;

- гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Учреждения, а также объема и состава обрабатываемых ПДн;

- научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

- специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляются должностными лицами, имеющими необходимые для этого квалификацию и опыт;

- наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы и могли быть оценены лицами, осуществляющими контроль;

- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

5. **Требования по организации безопасности информации в** информационной системе персональных данных

5.1. Учреждение принимает необходимые и достаточные меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

5.2. Ответственность за организацию обработки ПДн в Учреждении несет должностное лицо Учреждения, назначаемое приказом директора Учреждения.

5.3. Ответственный за организацию обработки ПДн в своей работе руководствуется инструкцией ответственного за организацию обработки персональных данных и другой защищаемой информации в Учреждении.

5.4. Учреждение осуществляет обработку ПДн без использования средств автоматизации, а также с использованием таких средств.

5.5. При обработке ПДн без использования средств автоматизации в Учреждении, в соответствии с положениями нормативных правовых актов в области обработки и защиты ПДн, реализует комплекс организационных и технических мер, обеспечивающих:

- обособление ПДн от информации, не содержащей ПДн;
- раздельную обработку и хранение каждой категории ПДн;
- соответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, установленным требованиям;
- соблюдение установленных требований при ведении журналов, содержащих ПДн, необходимые для однократного пропуска субъекта ПДн в помещения, занимаемые в Учреждение, или в иных аналогичных целях;
- сохранность материальных носителей ПДн;
- условия хранения, исключающие несанкционированный доступ к ПДн, а также смешение ПДн, обработка которых осуществляется в различных целях;
- надлежащее уточнение, уничтожение или обезличивание ПДн.

5.5. В соответствии с требованиями нормативных правовых актов в области обработки и защиты ПДн, обработки ПДн с использованием средств автоматизации в Учреждении создаются ИСПДн.

5.6. Все ИСПДн проходят периодическую классификацию и аттестацию в соответствии с требованиями нормативных правовых актов в области обеспечения безопасности ПДн.

5.7. Для каждой ИСПДн формируется модель угроз безопасности ПДн и на ее основе проводятся мероприятия по обеспечению безопасности информации в соответствии с требованиями, предъявляемыми к установленному классу ИСПДн.

5.8. Пересмотр моделей угроз для каждой ИСПДн осуществляется:

- в случае существенных изменений в инфраструктуре или порядке обработки ПДн в ИСПДн - в течение трех месяцев с даты фиксации изменений;
- в случае создания новой ИСПДн (выделения части из существующей ИСПДн) - в течение одного месяца с даты создания ИСПДн.

5.9. Обработка ПДн в Учреждении с использованием средств автоматизации ведется только в ИСПДн в Учреждении запрещается обработка ПДн с целями, не соответствующими целям создания ИСПДн, эксплуатация ИСПДн в составе, отличном от указанного при создании ИСПДн.

5.10. Ввод в эксплуатацию ИСПДн оформляется актом ввода в эксплуатацию и сопровождается аттестацией ИСПДн или декларированием соответствия ИСПДн требованиям по безопасности ПДн.

5.11. В целях обеспечения управления информационной безопасностью ПДн в Учреждении создается СЗПДн. Объектами защиты СЗПДн являются информация, обрабатываемая Учреждением и содержащая ПДн, а также инфраструктура, содержащая и поддерживающая указанную информацию.

5.12. СЗПДн реализуется комплексом правовых, режимных, организационных и программно-технических мер, которые включают:

- подготовку внутренних регулятивных документов Учреждения по вопросам обработки и защиты ПДн, контроль за исполнением в Учреждении требований нормативных правовых актов и внутренних регулятивных документов Учреждения в области обработки и защиты ПДн, а также внесение соответствующих изменений в имеющиеся внутренние регулятивные документы Учреждения;

- оформление письменных обязательств должностных лиц о неразглашении информации, обрабатываемой в информационных системах персональных данных Учреждения;

- доведение до сведения должностных лиц информации об установленных законодательством Российской Федерации санкциях за нарушения, связанные с обработкой и защитой ПДн;

- разработку и введение в действие внутренних регулятивных документов Учреждения по обеспечению информационной безопасности ИСПДн;

- регламентацию процедур создания и осуществление документирования действующих инженерных и информационных систем, программных комплексов, порядка внесения в них изменений и своевременной актуализации эксплуатационной документации;

- ознакомление должностных лиц с положениями нормативных правовых актов и внутренних регулятивных документов Учреждения в области обработки и защиты ПДн и организация обучения их правилам обработки и защиты ПДн;

- регламентацию обработки ПДн, в том числе хранения и передачи информации как внутри Учреждения, так и при взаимодействии с контрагентов Учреждения, государственными органами и организациями, обращения с документами и носителями, порядка их учета, хранения и уничтожения;

- установление правил доступа на объекты, в помещения, в ИС, применению в этих целях систем охраны и управления доступом;

- администрирования безопасности, мониторинга и аудита, управления доступом к защищаемым ресурсам;

- организацию технического оснащения объектов и ИСПДн в соответствии с существующими требованиями к информационной безопасности;

- формирование условий и технологических процессов обработки, хранения и передачи информации в Учреждении, обеспечивающих реализацию требований нормативных правовых актов, методических документов уполномоченных государственных органов и внутренних регулятивных документов Учреждения в области обработки и защиты ПДн;

- установление полномочий пользователей и форм представления информации пользователям ИСПДн;

- организацию непрерывного процесса контроля событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к защищаемой информации;

- организацию необходимых мероприятий с должностными лицами, а также собеседование с лицами, претендующими на работу в Учреждении;

- осуществление контроля эффективности организационных мер защиты;

- разработку защитных технических решений при стратегическом планировании архитектуры ИС, выборе технических средств обработки информации и при разработке и приобретении программного обеспечения.

5.10. Применение следующих компонентов программно-технических мер защиты:

- защищенных средств обработки информации, содержащей ПДн;

- системы криптографической защиты информации при ее передаче по каналам связи;

- межсетевых экранов для логического разделения подсетей и защиты от несанкционированного доступа из внешних информационных систем;

- аппаратных и программных средств защиты и контроля, устройств, технических систем и средств, используемых для обеспечения информационной безопасности, в том числе для обнаружения и нейтрализации попыток несанкционированного доступа к информации.

6. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

6.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

6.2. Учреждение несёт ответственность:

- за нарушение требований законодательства РФ по обработке и защите ПДн;

- за нарушение конфиденциальности обрабатываемых ПДн;

- за нарушение требований регулирующих организаций по обработке и защите ПДн.

6.3. Директор, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

6.4. Каждый сотрудник Учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

6.5. Сотрудники Учреждения, в соответствии со своими полномочиями владеющие ПДн сотрудников Учреждения, получающие и использующие их, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования ПДн.

6.6. Должностные лица, в обязанность которых входит ведение и учет ПДн, обязаны обеспечить каждому субъекту ПДн возможность ознакомления с документами и материалами, если иное не предусмотрено законом.

6.7. Неправомерный отказ в предоставлении собранных в установленном порядке ПДн, либо несвоевременное их предоставление в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации, влечёт наложение на должностных лиц административного наказания в порядке, установленном Кодексом Российской Федерации об административных правонарушениях.

6.8. В соответствии с Гражданским кодексом РФ лица, незаконными методами получившие информацию, составляющую ПДн, обязаны возместить причинённые убытки; такая же обязанность возлагается и на работников, не обладающих правом доступа к ПДн.

6.9. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконный сбор или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения, влечёт наложение наказания в порядке, предусмотренном Уголовным кодексом РФ.

6.10. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника, предусмотрена статьей 90 Трудового кодекса Российской Федерации № 197-ФЗ.

6.11. Неправомерность деятельности Учреждения по сбору и использованию ПДн может быть установлена в судебном порядке

7. Основные мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

7.1 Мероприятия по защите ПДн реализуются в Учреждении в следующих направлениях:

- предотвращение утечки информации, содержащей ПДн, по техническим каналам связи и иными способами;
- предотвращение несанкционированного доступа к содержащей ПДн информации, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;
- защита от вредоносных программ;
- обеспечение безопасного межсетевого взаимодействия;
- обеспечение безопасного доступа к сетям международного информационного обмена;
- анализ защищенности ИСПДн;

- обеспечение защиты информации с использованием криптографических средств при передаче ПДн по каналам связи;

- обнаружение вторжений и компьютерных атак;

- осуществления контроля за реализацией системы защиты ПДн.

7.2 Мероприятия по обеспечению безопасности ПДн включают в себя:

- реализацию разрешительной системы допуска пользователей к информационным ресурсам ИС и связанным с их использованием работам, документам;

- разграничение доступа пользователей ИСПДн и обслуживающих ИСПДн специалистов к информационным ресурсам, программным средствам обработки и защиты информации;

- регистрацию действий пользователей и обслуживающих ИСПДн специалистов, контроль несанкционированного доступа и действий пользователей и обслуживающих специалистов, а также третьих лиц;

- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

- предотвращение внедрения в ИС вредоносных программ и программных закладок, анализ принимаемой по информационно-телекоммуникационным сетям информации, в том числе на наличие компьютерных вирусов;

- ограничение доступа в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, содержащие ПДн;

- размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах контролируемой зоны;

- организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку ПДн;

- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

- реализацию требований по безопасному межсетевому взаимодействию ИС;

- использование защищенных каналов связи, защита информации при ее передаче по каналам связи;

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры ИС;

- обнаружение вторжений в ИС, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

- периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на ИС;

- анализ защищенности ИС с применением специализированных программных средств;

- централизованное управление системой защиты ПДн в ИС.

7.3. С целью поддержания состояния защиты ПДн на надлежащем уровне, в Учреждении, осуществляется внутренний контроль за

эффективностью системы защиты ПДн и соответствием порядка и условий обработки и защиты ПДн установленным требованиям. Внутренний контроль включает:

- мониторинг состояния технических и программных средств, входящих в состав СЗПДн;
- контроль соблюдения требований по обеспечению безопасности ПДн.

7.4. В целях осуществления внутреннего контроля в Учреждении проводятся периодические проверки условий обработки ПДн. Такие проверки осуществляются ответственным лицом за организацию обработки ПДн в Учреждении.

7.5. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывается директору Учреждения.