Политика безопасности обработки персональных данных в филиале АО «Татэнерго»- санатории-профилактории «Балкыш».

1. Область применения.

Настоящая Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, обрабатываемых в филиале АО «Татэнерго» - санатории – профилактории «Балкыш» (далее – Санаторий).

В Настоящей Политике определены требования к работникам Санатория, степень ответственности работников, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных Санатория.

Настоящая Политика разработана с учетом требований Конституции Российской Федерации, а также в соответствии с федеральными законами и подзаконными актами Российской Федерации, нормативными актами АО «Татэнерго», определяющими порядок обработки персональных данных, обеспечения безопасности и конфиденциальности такой информации.

Настоящая Политика разработана в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных в Санатории.

Положения настоящей Политики служат основой для разработки локальных нормативных актов Санатория, регламентирующих вопросы обработки и защиты персональных данных работников Санатория и других субъектов персональных данных, оператором которых является Санаторий.

Положения настоящей Политики являются обязательными для исполнения работниками Санатория, имеющими доступ к персональным данным.

2. Термины и определения.

В настоящем документе используются следующие термины и их определения.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение

(обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Доступ к информации – возможность получения информации и её использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

Информационная технология – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности персональных данных – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности персональных данных.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не распространять их без согласия субъекта персональных данных или наличия иного законного основания.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Объект вычислительной техники – стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации. К объектам вычислительной техники относятся автоматизированные системы, автоматизированные рабочие места, информационно-вычислительные центры и другие комплексы средств вычислительной техники. К объектам вычислительной техники могут быть отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

Оператор персональных данных – 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.

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

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

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

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты персональных данных.

Средство криптографической защиты информации – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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 ИСПДн.

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.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Сокращения.

В настоящем документе используются следующие сокращения.

Санаторий - филиал АО «Татэнерго» - санаторий-профилакторий «Балкыш».

ПДн - персональные данные.

ИСПДн - информационная система персональных данных.

ИБ - информационная безопасность.

СЗПДн - система защиты персональных данных.

4. Общие положения.

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

Информация и связанные с ней ресурсы должны быть доступны только для авторизованных пользователей. В ИСПДн должно осуществляться своевременное обнаружение угроз и реагирование на угрозы безопасности ПДн.

В ИСПДн необходимо исключить возможность преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Не допускается обработка персональных данных, несовместимая с целями сбора ПДн.

Санаторий использует ПДн для реализация договорных отношений, связи с Субъектом ПДн в случае необходимости направления уведомлений, информации и запросов, связанных с оказанием услуг, а также обработке заявлений, запросов и заявок Субъекта ПДн, улучшение качества услуг, оказываемых Санаторием.

Перечень ПДн, обрабатываемых в Санатории, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами АО «Татэнерго» с учетом целей обработки и защиты ПДн.

5. Условия обработки персональных данных.

Обработка ПДн в Санатории осуществляется с согласия Субъекта ПДн на обработку его ПДн, если иное не предусмотрено законодательством Российской Федерации в области ПДн.

Санаторий без согласия субъекта ПДн не раскрывает третьим лицам и не распространяет ПДн, если иное не предусмотрено федеральным законом.

Санаторий несёт ответственность за нарушение норм, регулирующих обработку и защиту ПДн в соответствии с федеральными законами.

6. Перечень действий с персональными данными и способы их обработки.

Санаторий осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение ПДн. Обработка ПДн в Санатории осуществляется как без использования средств автоматизации, так и с использованием средств автоматизации.

Работники, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законодательством.

ПДн могут быть предоставлены Санаторием органам государственной власти и местного самоуправления в порядке, установленном законодательством, а также другим организациям, согласно условиям договоров с соблюдением требований законодательства РФ по защите ПДн.

Передача ПДН осуществляется с соблюдением следующих требований:

- не сообщать ПДН третьей стороне без письменного согласия Субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта ПДн, а также в других случаях, предусмотренных федеральным законодательством;
- не сообщать ПДн в коммерческих целях без письменного согласия Субъекта ПДн;
- предупредить лиц, получающих 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, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на передачу ПДн в порядке, установленном федеральными законами.

Ответственность за уничтожение носителей ПДн, в том числе черновиков и проектов документов их содержащих, несут исполнители, которые работают с данными носителями информации. Документ считается уничтоженным, если содержащиеся в нем персональные данные не подлежат восстановлению и не могут быть идентифицированы. Документы, содержащие ПДн, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации. Уничтожение ПДн, утративших свое практическое значение и не имеющих исторической ценности, производится по акту.

Безопасность ПДн, обрабатываемых в Санатории, обеспечивается реализацией правовых, организационных и технических мер, необходимых для обеспечения требований федерального законодательства в области защиты ПДн. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение,

изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

Для предотвращения несанкционированного доступа к ПДн применяются следующие организационно-технические меры:

- ограничение состава лиц, имеющих доступ к ПДн;
- разграничение доступа пользователей к информационным ресурсам и
- программно-аппаратным средствам обработки информации;
- определение угроз безопасности ПДн при их обработке,
- формирование на их основе моделей угроз;
- разработка на основе модели угроз системы защиты ПДн;
- регистрация и учет действий пользователей информационных систем ПДн;
- использование антивирусной защиты;
- применение, в необходимых случаях, средств межсетевого экранирования, обнаружения вторжений, анализа защищенности и средств криптографической защиты информации.

Все работники Санатория, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению установленного режима безопасности ПДн.

При вступлении в должность нового работника непосредственный руководитель структурного подразделения обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Работник должен быть ознакомлен с настоящей Политикой, установленными процедурами работы с элементами ИСПДн и СЗПДн.

Работники Санатория, использующие технические средства аутентификации, должны обеспечивать сохранность персональных идентификаторов (электронных ключей) и не допускать несанкционированный доступ к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Работники Санатория должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства идентификации и аутентификации).

Работники Санатория должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи ИСПДн должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Работникам запрещается разглашать защищаемую информацию, которая стала им известна в силу выполнения ими своих должностных обязанностей.

При работе с ПДн в ИСПДн работники Санатория обязаны исключить возможность просмотра ПДн третьими лицами с мониторов объектов вычислительной техники.

При завершении работы с ИСПДн работники обязаны защитить объекты вычислительной техники с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Работники Санатория должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, нарушающих принятые политику и процедуры безопасности ПДн.

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

7. Заключительные положения.

Настоящая Политика подлежит размещению на официальном сайте Санатория.

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и нормативных документов по обработке и защите ПДн.