УТВЕРЖДЕНЫ
Приказом
ООО «Газпром межрегионгаз Тула»
от «3» ноября 2011 № 61

Требования по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Газпром межрегионгаз Тула»

г.Тула

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ПДн	Персональные данные
СрЗИ	Средство защиты информации
СЗПДн	Система защиты персональных данных
ФСТЭК России	Федеральная служба по техническому и экспортному контролю России

1. Общие положения

1.1. Назначение

Настоящие Требования по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – Требования) определяют обязательные требования и правила по обеспечению безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) ООО «Газпром межрегионгаз Тула», в том числе при передаче/получении в/из сторонние организации, а также физическим лицам (субъектам персональных данных).

Требования разработаны на основании нормативно-правовых актов и методических документов по защите ПДн, перечисленных в разделе 5.

Настоящие Требования не отменяют требования иных документов, регламентирующих порядок обращения с информацией ограниченного доступа, не содержащей сведений, составляющих государственную тайну (конфиденциальной информацией).

Требования допускают внесение изменений, вызванных дополнениями (изменениями) нормативно-правовой основы, развитием ИСПДн или изменением условий обработки ПДн. Требования и изменения к ним вводятся в действие приказом генерального директора ООО «Газпром межрегионгаз Тула» и вступают в силу с момента подписания приказа.

1.2. Целевая аудитория

Настоящие Требования предназначены для сотрудников подразделений ООО «Газпром межрегионгаз Тула» (далее – Общества), непосредственно связанных с эксплуатацией ИСПДн и обеспечением безопасности ПДн, руководителей данных подразделений, а так же для сотрудников сторонних организаций, допускаемых в установленном порядке к выполнению работ на оборудовании ИСПДн, в т.ч. по модернизации оборудования и программного обеспечения данной системы.

2. Принципы защиты персональных данных

Обеспечение безопасности ПДн при их обработке в ИСПДн осуществляется путем выполнения комплекса организационных и технических мероприятий (применения технических средств) в рамках системы (подсистемы) защиты персональных данных (СЗПДн), развертываемой в ИСПДн в процессе ее создания или модернизации.

При создании СЗПДн должны использоваться принципы и выполняться требования, приведенные в настоящих Требованиях.

Обеспечение безопасности ПДн в ИСПДн представляет собой непрерывный во времени управляемый процесс и осуществляется в соответствии со следующими принципами:

– законность;
– комплексность;
– системность;
– непрерывность;
– своевременность;
– преемственность и совершенствование;
– разумная достаточность;
– простота применения средств защиты;
– обоснованность;
– персональная ответственность;
– минимизация привилегий (полномочий);
– взаимодействие и сотрудничество.

Сущность перечисленных принципов изложена в приложении.

На основе данных принципов строятся две основные группы требований по обеспечению безопасности ПДн при их обработке в ИСПДн:

– организационные требования;
– технические требования.

3. Организационные требования

3.1. Требования по организационно-штатному обеспечению

Для эксплуатации СЗПДн, выполнения мероприятий по обеспечению безопасности ПДн и осуществления контроля их выполнения, приказом генерального директора Общества создается подразделение обеспечивающее безопасность ПДн (п. 13 «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства РФ № 781 от 17.11.2007 г., п. 1.3 «Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного приказом ФСТЭК России № 58 от 05.02.2010 и пп. 3.2., 5.6.3., 6.3.3., 6.3.11. «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утвержденных Гостехкомиссией (ФСТЭК) России, 2002 г.).

Сотрудники данного подразделения ответственные за обеспечение безопасности ПДн должны иметь высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и пройти переподготовку или повышение квалификации по вопросам технической защиты информации.

Положение о подразделении разрабатывается на основе действующего трудового законодательства и законодательства о защите персональных данных. Должностные инструкции для сотрудников подразделения разрабатываются на основе Единого квалификационного справочника должностей руководителей, специалистов и служащих (Раздел справочника «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации», утвержденный приказом № 205 Министерства здравоохранения и социального развития РФ от 22.04.2009 г.).

3.2. Требования по подготовке персонала

Персонал Общества, допускаемый к обработке ПДн в ИСПДн, должен быть подготовлен к работе с ПДн с использованием средств информационной системы и средств защиты информации (СрЗИ). Обязательным условием допуска является изучение организационно-распорядительных документов Общества по обеспечению безопасности ПДн.

Персонал, осуществляющий эксплуатацию СрЗИ в составе ИСПДн должен дополнительно изучить эксплуатационные документы на средства и получить необходимые навыки работы с этими средствами в составе ИСПДн.

3.3. Требования по материально-техническому обеспечению

При эксплуатации СЗПДн должно осуществляться непрерывное и всестороннее материально-техническое обеспечение, включающее в себя:

– поставку необходимого оборудования и расходных материалов;

– обновление лицензий на программное обеспечение;

– обновление версий используемого программного обеспечения и СрЗИ, и при необходимости увеличение их количества и создание резерва данных средств;

– финансирование подготовки специалистов на курсах по обеспечению безопасности информации.

3.4. Требования по организационно-правовому обеспечению

В целях организационно-правового обеспечения деятельности по защите ПДн при их обработке в ИСПДн должна быть создана необходимая организационно-распорядительная база, к разработке и/или согласованию которой могут быть привлечены лицензиаты ФСТЭК России.

Указанная организационно-распорядительная база должна периодически актуализироваться с учетом изменения характера угроз информационной безопасности, расположения, конфигурации, режима функционирования и особенностей обработки ПДн в ИСПДн, в том числе организационных, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в ИСПДн.

3.5. Требования к организации доступа к персональным данным

Доступ сотрудников Общества к ПДн, обрабатываемым в ИСПДн, должен быть ограничен. Предоставление доступа осуществляется в соответствии с организационно-распорядительными документами Общества.

Лица, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании списка, утвержденного генеральным директором Общества. Данный список поддерживается в актуальном состоянии ответственным за обеспечение безопасности ПДн.

Пользователи ИСПДн и СрЗИ обязаны:

– не разглашать информацию, к которой они допущены, в том числе сведения о СрЗИ, ключевых документах и других мерах защиты;

– соблюдать требования по обеспечению безопасности ПДн, предусмотренные организационно-распорядительной и эксплуатационной документацией.

4. Технические требования

4.1. Соответствие действующему законодательству в области защиты персональных данных

Технические меры по обеспечению безопасности ПДн должны применяться в соответствии с положениями нормативно-правовых актов Российской Федерации и методических документов уполномоченных федеральных органов исполнительной власти в сфере защиты ПДн при их обработке в ИСПДн.

Обеспечение безопасности обработки ПДн с использованием СрЗИ организуют и обеспечивают сотрудники Общества, а также лица, которым на основании договора поручается обработка ПДн, и/или лица, которым на основании договора поручается оказание услуг по организации и обеспечению безопасности обработки ПДн.

Обеспечение функционирования СрЗИ возлагается на подразделение обеспечивающее безопасность персональных данных.

4.2. Требования по защите от угроз несанкционированного доступа

В ИСПДн должны приниматься меры по исключению несанкционированного доступа (НСД) к ПДн, в т.ч. НСД в результате действий непреднамеренного характера.

Меры по исключению НСД к ПДн должны быть реализованы на основе:

– ограничения физического доступа к элементам ИСПДн;

– реализации разрешительной системы доступа к ПДн и сервиса контроля доступа на уровне пользователей с применением встроенных средств информационных и операционных систем, службы каталогов, а так же дополнительных средств идентификации;

– использования сертифицированных СрЗИ;

– регистрации и анализа информации о событиях (в т.ч. событиях доступа к ИСПДн и доступа к ПДн);

– антивирусной защиты рабочих станций в целях противодействия распространению шпионского программного обеспечения, используемого для реализации НСД;

– контроля и анализа защищенности с целью превентивного определения фактического уровня обеспечения информационной безопасности в ИСПДн.

4.3. Требования по защите от угроз доступности информационных ресурсов

В целях обеспечения доступности информационных ресурсов ИСПДн на уровне СЗПДн должны приниматься дополнительные меры, включая (но не ограничиваясь):

– резервное копирование и восстановление информации;

– применение СрЗИ в отказоустойчивой конфигурации;

– ведение двух копий программных СрЗИ и их периодическое обновление;

– применение дополнительных функций мониторинга, встроенных в средства межсетевого экранирования.

4.4. Требования к управлению информационной безопасностью

СрЗИ, применяемые в СЗПДн, по возможности должны иметь возможность централизованного и удаленного управления.

При решении задач управления СЗПДн должны решаться следующие вопросы:

– распределение функций управления доступом к данным и их обработкой между должностными лицами;

– определение порядка изменения правил доступа к защищаемой информации;

– определение порядка изменения правил доступа к резервируемым информационным ресурсам;

– определение порядка действий должностных лиц в случае возникновения нештатных ситуаций;

– определение порядка проведения контрольных мероприятий и действий по результатам их выполнения.

4.5. Требования по физической безопасности информационной системы персональных данных

Физическая безопасность ИСПДн должна обеспечиваться с целью контроля доступа в помещения с элементами ИСПДн посторонних лиц, наличия надежных препятствий от несанкционированного проникновения в помещения и в хранилища носителей информации, особенно в нерабочее время.

В целях обеспечения непрерывного устойчивого функционирования ИСПДн должны быть приняты меры по противопожарной защите помещений, осуществлению бесперебойного электропитания оборудования ИСПДн и поддержанию требуемого температурно-влажностного режима окружающей среды.

4.6. Способы приема (передачи) персональных данных и предъявляемые требования по обеспечению безопасности

Для реализации обмена ПДн в ИСПДн возможны следующие способы:

– передача (прием) ПДн с использованием выделенных каналов передачи данных;

– передача (прием) ПДн с использованием съемных носителей информации;

– передача (прием) ПДн с использованием сети общего пользования;

– передача (прием) ПДн без использования средств автоматизации.

4.6.1. Требования по обеспечению безопасности ПДн, передаваемых (получаемых) с использованием выделенных каналов передачи данных

Для обеспечения безопасности при обмене ПДн с использованием выделенных каналов передачи данных, необходимо выполнение следующих требований:

– передача данных осуществляется с привлечением провайдера телекоммуникационных услуг, имеющего лицензии и сертификаты, подтверждающие право оказания услуг при работе с информацией ограниченного доступа класса не ниже, установленного для ИСПДн, либо с использованием доверенных каналов (Multi-protocol label switching) и/или точка-точка (Point-to-point tunneling protocol). В противном случае необходимо применять сертифицированные средства криптографической защиты;

– подключение сторонних организаций к сети ИСПДн осуществляется через сертифицированные межсетевые экраны;

– применение средств антивирусной защиты при приеме/передаче ПДн из/в сторонние организации.

4.6.2. Требования по обеспечению безопасности ПДн, передаваемых (получаемых) с использованием съемных носителей

Для обеспечения безопасности при обмене ПДн с использованием съемных носителей, необходимо выполнение следующих требований:

– применение средств антивирусной защиты при приеме/передаче ПДн из/в сторонние организации, к полученной со съемных носителей информации (включая клиентские и серверные вычислительные средства), с предварительной проверкой данных на съемных носителях (на предмет наличия вредоносных программ);

– при необходимости полученная/переданная информация должна сопровождаться копией передаваемых ПДн на бумажном носителе, заверенной подписью ответственного лица и печатью организации, предоставляющей информацию.

4.6.3. Требования по обеспечению безопасности ПДн, передаваемых (получаемых) с использованием сети общего пользования

Для обеспечения безопасности при обмене ПДн с использованием сети общего пользования (Интернет), необходимо выполнение следующих требований:

– подключение субъектов к сети ИСПДн осуществляется через сертифицированные межсетевые экраны;

– применение средств антивирусной защиты при приеме/передаче ПДн;

– использование шифрования данных с применением сертифицированных средств криптографической защиты и/или использование электронной цифровой подписи (сформированной с использованием сертифицированных криптографических средств), с применением механизма доказательства подписи.

4.6.4. Требования по обеспечению безопасности ПДн, передаваемых (получаемых) без использования средств автоматизации

При получении данных от субъектов (организаций, физических лиц) без использования средств автоматизации необходимо выполнение следующих требований:

– получение у субъекта, передающего ПДн расписку об использовании ПДн с обозначенными целью сбора информации и временем использования ПДн.

По первому требованию субъекта ПДн, необходимо предоставить ему в полученном объеме сведения о его ПДн.

При передаче ПДн с использованием средств факсимильной связи или почтой, необходимо сопровождать их сопроводительным письмом с указанием кому они направляются и от кого, а так же письмо должно содержать следующий текст: «При получении данных сведений, содержащих персональные данные, *получившее Учреждение* обязано обеспечить конфиденциальность этих сведений в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ст. 3 Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания).

В случае достижения цели обработки персональных данных *получившее Учреждение* обязано незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных (ст. 21 Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»).

5. Нормативно-правовые акты и методические документы по защите персональных данных при их обработке в информационных системах персональных данных

При подготовке настоящих Требований использованы следующие нормативно-правовые акты и методические документы по защите персональных данных при их обработке в информационных системах персональных данных:

1. Федеральный закон от 27.07.2006. «Об информации, информационных технологиях и о защите и информации» № 149-ФЗ
2. Федеральный закон от 27.07.2006 «О персональных данных» № 152-ФЗ
3. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное Постановлением Правительства РФ от 17.11.2007 № 781;
4. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное постановлением Правительства Российской Федерации № 687 от 15 сентября 2008 г.
5. Порядок проведения классификации информационных системах персональных данных, утвержденный приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20
6. Положение о методах и способах защиты информации в информационных системах персональных данных, утверждено приказом ФСТЭК России от 05.02.2010 № 58
7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.2008.
8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 14.02.2008.
9. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждены приказом Гостехкомиссии России от 30.08.2002 № 282

Приложение 1

Принципы обеспечения безопасности ПДн

Законность. Обеспечение безопасности ПДн в ИСПДн должно осуществляться в соответствии с положениями и требованиями существующих законов, стандартов и нормативно-методических документов в области информации, информатизации и защиты информации и нормативными документами Общества.

Комплексность. При обеспечении безопасности ПДн в ИСПДн согласованно применяются разнородные механизмы обеспечения информационной безопасности. Обеспечение безопасности информационных ресурсов осуществляется в течение всего их жизненного цикла, на всех технологических этапах их обработки (преобразования) и использования, во всех режимах функционирования.

Системность. При обеспечении безопасности ПДн в ИСПДн учитываются все взаимосвязанные, взаимодействующие и изменяющиеся во времени элементы, условия и факторы, существенно значимые для понимания и решения проблемы обеспечения информационной безопасности.

Непрерывность. Обеспечение безопасности ПДн в ИСПДн не является разовым мероприятием по защите информации или простой совокупностью проведенных мероприятий и установленных средств защиты информации, а представляет собой непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

Своевременность. Меры безопасности ПДн в ИСПДн носят упреждающий характер.

Преемственность и совершенствование. Обеспечение безопасности ПДн в ИСПДн должно осуществляться при постоянном совершенствовании мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн с учетом изменений в методах и средствах нарушения информационной безопасности, нормативных требований по защите, достигнутого мирового опыта в этой области.

Разумная достаточность (экономическая целесообразность, сопоставимость возможного ущерба и затрат). Уровень затрат на обеспечение безопасности ПДн в ИСПДн должен быть адекватным ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения, искажения ПДн и снижения качества сервисов ИСПДн.

Простота применения средств защиты. Механизмы обеспечения безопасности ПДн в ИСПДн должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей.

Обоснованность. Меры и средства защиты должны быть обоснованными с точки зрения заданного уровня безопасности и соответствовать установленным требованиям и нормам.

Персональная ответственность. Ответственность за обеспечение безопасности ПДн в ИСПДн должна возлагаться на каждого работника Общества, допущенного к работе с системой (ПДн), в пределах его полномочий.

Минимизация привилегий (полномочий). Пользователям и персоналу Общества, эксплуатирующим ИСПДн, должны предоставляться минимальные права доступа в соответствии с производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

Взаимодействие и сотрудничество. В Обществе должна быть создана благоприятная атмосфера, в которой работники должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделений, на которые возложены обязанности по обеспечению безопасности ПДн.