Приложение к приказу
ООО «Газпром межрегионгаз Тамбов»
от «9» июня 2025 года № 90

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в ООО «Газпром межрегионгаз Тамбов»

Тамбов

ОГЛАВЛЕНИЕ

1. Термины, определения и сокращения

В настоящем Положении об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в ООО «Газпром межрегионгаз Тамбов» (далее – Положение) используются сокращения, термины и определения, приведенные в пп. 1.1 и 1.2.

1.1. Используемые сокращения

Общество, оператор – ООО «Газпром межрегионгаз Тамбов».

ПД – персональные данные.

ИБ – информационная безопасность.

ЛНА – локальные нормативные акты.

ИСПД – информационная система персональных данных.

СЗПД – система защиты персональных данных.

ОКЗ – отдел корпоративной защиты Общества.

ПСЭ – структурное подразделение Общества, осуществляющее сопровождение эксплуатации ИСПД.

ОИТТиС – отдел информационных технологий, телекоммуникаций и связи.

ЭСОД – электронная система обмена данными.

1.2. Используемые термины и определения

Владелец ИСПД – структурное подразделение Общества, выступающее постановщиком (функциональным заказчиком) реализуемых с использованием ИСПД задач.

Информационные системы персональных данных – совокупность содержащихся в базах данных ПД и обеспечивающих их обработку информационных технологий и технических средств.

Машинные носители ПД – входящие в состав ИСПД носители информации (жесткие диски), на которых хранятся ПД, обрабатываемые в ИСПД, а также внешние носители ПД (ленточные кассеты, оптические диски, флеш-накопители, дискеты и прочие), на которых хранятся ПД, извлечённые из ИСПД.

Модель нарушителя безопасности ПД – совокупность предположений о возможностях, которые могут использоваться при создании способов подготовки и проведения атак.

Модель угроз безопасности ПД – перечень возможных угроз безопасности ПД.

Носитель информации – материальный объект, предназначенный для записи и хранения информации.

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

Пользователь ИСПД – лицо или группа лиц, использующих ИСПД в ходе выполнения своих функциональных обязанностей.

Процесс обеспечения информационной безопасности – совокупность

процедур, выполняемых работниками структурных подразделений, направленная на обеспечение защиты информации (данных) от утечки, хищения, утраты, несанкционированного доступа, а также иных неправомерных действий.

Угрозы безопасности ПД – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного доступа к ПД, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПД, а также иные неправомерные действия при их обработке в ИСПД.

Уровень защищенности ПД – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПД при их обработке в ИСПД.

Функциональный заказчик - структурное подразделение Общества, определяющее перечень требований к созданию и функционированию ИСПД.

2. Общие положения

2.1. Настоящее Положение разработано в соответствии с нормативными правовыми актами Российской Федерации и ЛНА ПАО «Газпром» и ООО «Газпром межрегионгаз», регламентирующими вопросы обработки и защиты ПД.

2.2. Положение определяет порядок организации и проведения работ по защите ПД, обрабатываемых в ИСПД, эксплуатируемых в Обществе.

2.3. Задачей настоящего Положения является определение:

порядка обеспечения защиты ПД на этапах жизненного цикла ИСПД;

порядка осуществления контроля за соблюдением требований ИБ;

прав и обязанностей работников Общества, связанных с обеспечением ИБ на этапах жизненного цикла ИСПД.

2.4. Этапы жизненного цикла ИСПД включают в себя:

формирование требований к ИСПД;

проектирование, разработку, внедрение ИСПД;

ввод ИСПД в эксплуатацию;

эксплуатацию ИСПД;

вывод ИСПД из эксплуатации.

2.5. В Положении не рассматриваются вопросы обеспечения безопасности ПД, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

3. Принципы обеспечения безопасности ПО при их обработке в ИСПД

3.1. Обеспечение безопасности ПД в ИСПД реализуется в рамках СЗПД, создаваемой в соответствии с Требованиями к защите ПД при их обработке в ИСПД, утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119.

3.2. СЗПД включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПД и информационных технологий, используемых в ИСПД.

Неиспользованную календарных

При определении типа угроз безопасности ПД, актуальных для ИСПД, в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ (далее – Закон «О персональных данных»), учитывается оценка вреда, который может быть причинен субъектам ПД. Это позволяет соотнести указанный вред и адекватность принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом «О персональных данных».

Оценка вреда осуществляется по следующим критериям:

вред отсутствует или является несущественным – последствия реализации угроз безопасности ПД не ущемляют права и свободы субъекта ПД, в том числе права на неприкосновенность частной жизни, на личную и семейную тайну;

существенный вред – последствия реализации угроз безопасности ПД ущемляют права и свободы субъекта ПД, в том числе права на неприкосновенность частной жизни, на личную и семейную тайну.

При определении типа актуальных угроз безопасности ПД угрозы безопасности ПД, реализация которых не может нанести существенного вреда субъектам ПД, считаются неактуальными.

3.3. Выбор средств защиты информации для СЗПД осуществляется в соответствии с приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3.4. В случае если безопасность ПД обеспечивается мерами, связанными с использованием средств криптографической защиты информации, состав, содержание и порядок применения таких мер определяется в соответствии с требованиями приказа ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

3.5. Перечень требований к материальным носителям биометрических ПД и технологиям хранения таких данных вне ИСПД формируется в соответствии с постановлением Правительства Российской Федерации от 06 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

3.6. Для эксплуатируемых в Обществе ИСПД, для которых в процессе их создания не были предусмотрены меры по обеспечению безопасности ПД, владельцем ИСПД организуется проведение комплекса организационных и технических мероприятий по разработке и внедрению СЗПД.

3.7. К работам по созданию, модернизации ИСПД, внедрению и эксплуатации входящих в ее состав средств защиты информации на договорной основе могут привлекаться юридические лица и индивидуальные предприниматели,

имеющие лицензии на осуществление соответствующих видов деятельности.

4. Формирование требований к ИСПД

4.1. Основаниями для создания (модернизации) ИСПД, в частности, являются:

требования законодательства Российской Федерации;

требования нормативных документов ПАО «Газпром»;

требования нормативных документов ООО «Газпром межрегионгаз»;

требования ЛНА Общества;

приказы Общества, распоряжения руководства Общества;

условия заключаемых Обществом договоров.

4.2. Решение о целесообразности начала работ по созданию ИСПД принимает руководство Общества на основании предложений руководителей структурных подразделений.

4.3. Требования к СЗПД формируются на основе обследования ИСПД в соответствии с методикой СТО Газпром 4.2-3-006-2014.

4.4. В результате обследования определяются следующие исходные данные:

сведения об ИСПД и вычислительной инфраструктуре, в рамках которой она функционирует (структурно-функциональные характеристики, применяемые информационные технологии, особенности функционирования, перечень технических средств, названия и версии системного и прикладного программного обеспечения, наличие и характер межсетевых взаимодействий, места размещения составных частей, а также прочая информация, оказывающая влияние на функционирование ИСПД);

перечень носителей информации, используемых для хранения биометрических ПД вне ИСПД;

перечни лиц или категорий лиц, осуществляющих обработку ПД в ИСПД, имеющих доступ к обрабатываемым ПД (пользователи ИСПД и работники, обеспечивающие эксплуатацию ИСПД);

категории ПД, обрабатываемых в ИСПД (специальные, биометрические, общедоступные, иные);

категории субъектов ПД, сведения о которых обрабатываются в ИСПД (субъекты, являющиеся работниками оператора ПД; субъекты, не являющиеся работниками оператора ПД);

количество субъектов ПД, не являющихся сотрудниками оператора, сведения о которых обрабатываются в ИСПД (менее 100 000, более 100 000);

условия и (или) сроки прекращения обработки ПД.

4.5. На основании полученных исходных данных определяются:

актуальные угрозы безопасности ПД и их тип;

уровень защищенности ПД;

перечень требований к защите ПД, исполнение которых обеспечивает уровень защищенности ПД, в том числе требования к материальным носителям биометрических ПД.

4.5.1. Определение актуальности угроз безопасности ПД выполняется в соответствии с нормативными документами уполномоченных федеральных органов исполнительной власти и СТО Газпром 4.2-0-005-2014.

4.5.2. Сформированный перечень актуальных угроз безопасности ПД и их тип включается в модель угроз безопасности ПД.

4.5.3. Уровень защищенности ПД фиксируется в акте определения уровня защищенности ПД при их обработке в ИСПД (далее – Акт). Акт готовится владельцем ИСПД и передается на рассмотрение комиссии по защите информации вместе с результатами обследования ИСПД и моделью угроз безопасности ПД. Акт утверждается генеральным директором Общества (или иным уполномоченным лицом). Форма Акта приведена в Приложении № 1.

4.6. Требования к обеспечению безопасности ПД задаются в техническом задании на создание ИСПД (п. 4.6 СТО Газпром 4.2-3-001-2009).

4.7. Для эксплуатируемых в Обществе ИСПД, для которых в процессе их создания не были предусмотрены меры по обеспечению безопасности ПД, требования к обеспечению безопасности ПД формируются в документе «Перечень требований к СЗПД и состав мер по обеспечению безопасности ПД при их обработке в ИСПД» (Приложение № 2).

5. Проектирование, разработка, внедрение ИСПД

5.1. На этапе разработки проектной документации на ИСПД формируется комплект документов, включающий в себя:

материалы с результатами обследования ИСПД;

схема функциональной структуры ИСПД и СЗПД;

модель угроз безопасности ПД;

модель нарушителя безопасности ПД (разрабатывается в случае использования в СЗПД криптографических средств защиты информации);

акт определения уровня защищенности ПД при их обработке в ИСПД;

обоснование определения базового набора защитных мер, его адаптации, уточнения и дополнения, а также обоснование применения компенсирующих защитных мер (п. 9 приказа ФСТЭК России от 18 февраля 2013 г. № 21);

параметры и настройки программных и технических средств СЗПД, функционирование которых обеспечивает реализацию мер по обеспечению безопасности ПД;

эксплуатационную документацию на ИСПД, в том числе СЗПД;

матрицу доступа к ИСПД (если ведение матрицы осуществляется не в электронном виде, а в форме документа на бумажном носителе);

для применяемых средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации, – документы, подтверждающие соответствие требованиям.

5.2. Допускается включение перечисленных в п. 5.1 документов в состав проектной и эксплуатационной документации на ИСПД, в том числе в виде соответствующих разделов, а также объединение в одном комплекте документов данных о нескольких СЗПД ИСПД.

5.3. В случае если сведения, указанные в п. 5.1, документируются в рамках других процессов системы обеспечения информационной безопасности Общества, допускается ссылка на указанные документы.

6. Ввод ИСПД в эксплуатацию

6.1. На этапе ввода ИСПД в эксплуатацию организуется проведение оценки эффективности реализованных в рамках СЗПД мер по обеспечению безопасности ПД.

6.2. Оценка эффективности применяемых в СЗПД мер защиты информации может проводиться в форме:

- приемочных испытаний ИСПД;
- проверки выполнения требований обеспечения безопасности ПД при их обработке в ИСПД с оформлением соответствующего акта (уполномоченной комиссией Общества, либо внешней организацией, имеющей соответствующие разрешительные документы, в соответствии с договором подряда);
- аттестации ИСПД (требования для аттестации разрабатываются в соответствии с законодательством Российской Федерации, СТО Газпром, ЛНА ПАО «Газпром», ООО «Газпром межрегионгаз» и Общества).

6.3. Выявленные в ходе оценки эффективности принимаемых мер по обеспечению безопасности ПД недостатки, влекущие за собой риски нарушения установленных законодательством Российской Федерации и Положением требований, должны быть устранены. Если устранение недостатков не может быть выполнено незамедлительно, то эксплуатация ИСПД должна быть приостановлена.

6.4. Эксплуатация ИСПД разрешается только после успешной оценки эффективности принимаемых мер по обеспечению безопасности ПД. Оценка оформляется актом (Приложение № 3).

6.5. Основанием для ввода ИСПД в эксплуатацию является приказ генерального директора Общества.

7. Эксплуатация ИСПД

7.1. В ходе эксплуатации ИСПД организуется выполнение следующих процедур процесса обеспечения информационной безопасности ПД:

резервное копирование ПД;

восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

удаление или обезличивание ПД, в отношении которых: цель обработки достигнута; сроки обработки, указанные в согласии субъекта ПД на обработку его ПД, истекли; обработка должна быть прекращена в связи с отзывом субъектом ПД согласия на обработку его ПД, если иное не предусмотрено законодательством Российской Федерации;

контроль за соблюдением допустимых сроков и условий обработки ПД в ИСПД с целью своевременного удаления или обезличивания указанных ПД;

учет машинных носителей ПД первого и второго уровня защищенности, установленных пп. 9, 10 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных

постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, их безопасное хранение и уничтожение;

обнаружение фактов несанкционированного доступа к ПД и их расследование;

учет и управление доступом пользователей к ПД, обрабатываемым в ИСПД;

выявление условий, определяющих необходимость модернизации СЗПД;

контроль за принимаемыми мерами по обеспечению безопасности ПД, обрабатываемых в ИСПД, и уровнем защищенности ПД.

7.1.1. Для обеспечения возможности восстановления ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним, возникновения неисправности аппаратной или программной части ИСПД, иных форс-мажорных обстоятельств, должно осуществляться резервное копирование ПД, обрабатываемых в ИСПД. Резервное копирование ПД осуществляется в порядке, установленном ЛНА Общества.

7.1.2. Контроль сроков обработки ПД в ИСПД осуществляется в порядке, установленном ЛНА Общества.

ПД, цель обработки которых достигнута, должны быть удалены из ИСПД или обезличены. Факт удаления ПД отражается в порядке, установленном ЛНА Общества.

При восстановлении ПД из резервной копии должно быть проведено удаление из ИСПД ПД, которые в ней ранее обрабатывались, но были удалены в связи с прекращением их обработки.

7.1.3. В отношении машинных носителей ПД устанавливается следующий порядок учета, хранения и уничтожения:

машинные носители ПД должны быть учтены в порядке, установленном ЛНА Общества;

внешние носители ПД, в том числе применяемые для резервного копирования, а также аппаратные средства ИСПД, содержащие машинные носители ПД, должны размещаться в специализированных помещениях, в отношении которых принимаются установленные в Обществе меры физической защиты.

7.1.4. Обнаружение и расследование фактов несанкционированного доступа к ПД, обрабатываемым в ИСПД, должно осуществляться в рамках действующего в Обществе порядка проведения служебных проверок.

7.2. К ПД, обрабатываемым в ИСПД, допускаются только лица, занимающие должности, включенные в перечень должностей, замещение которых предусматривает осуществление обработки персональных данных (далее – Перечень). Порядок предоставления/отзыва прав доступа работников Общества к ИСПД регламентируется ЛНА Общества.

7.3. В ходе эксплуатации ИСПД проводится контроль условий, определяющих необходимость модернизации СЗПД.

7.4. Необходимость проведения модернизации СЗПД определяется в случае изменения:

категорий ПД, обрабатываемых в ИСПД, и/или категорий и количества субъектов, ПД которых обрабатываются в ИСПД;

перечня и/или актуальности угроз безопасности ПД;

структурно-функциональных характеристик ИСПД, применяемых в ней информационных технологий или особенностей ее функционирования (в том числе состава или структуры программного обеспечения, технических средств обработки ПД, топологии ИСПД, места размещения ИСПД или ее составных частей);

требований законодательства Российской Федерации в области защиты ПД, устанавливающих необходимость внесения изменений в СЗПД.

7.5. На этапе эксплуатации ПСЭ осуществляется хранение комплекта документации на ИСПД, разработанной на этапе проектирования системы. Копия документации на ИСПД хранится в ГКЗ.

8. Особенности эксплуатации ИСПД сторонних организаций

8.1. При подключении к ИСПД, владельцами которых выступают сторонние организации, в частности системам дистанционного банковского обслуживания, системам передачи отчетности в государственные органы и учреждения, требования к безопасности ПД определяются владельцами данных ИСПД в соответствующем договоре, в эксплуатационной документации и иных нормативных документах, регламентирующих работу в ИСПД.

8.2. Передача ПД в сторонние организации осуществляется только при наличии согласия субъекта ПД или иных правовых оснований для такой передачи.

8.3. Работа с ИСПД кредитных организаций, государственных и муниципальных учреждений (ЭСОД) осуществляется в соответствии с требованиями настоящего Положения и Инструкции по обеспечению ИБ на этапах жизненного цикла электронных систем обмена данными ООО «Газпром межрегионгаз Тамбов» с кредитными организациями, государственными и муниципальными учреждениями (далее – Инструкция ЭСОД).

8.4. Для обрабатывающих ПД информационно-управляющих систем (ИУС) ООО «Газпром межрегионгаз» (ПАО «Газпром»), внедряемых в Обществе по типовым проектным решениям, Общество:

принимает участие в разработке и согласовании документов на ИСПД, в том числе на СЗПД;

обеспечивает выполнение организационных и технических требований по защите ПД ИУС при доступе работников Общества к ИУС ООО «Газпром межрегионгаз» (ПАО «Газпром»);

участвует в расследовании фактов несанкционированного доступа к ПД, обрабатываемых в ИСПД;

информирует Управление корпоративной защиты ООО «Газпром межрегионгаз» о начале работ по созданию (модернизации) ИСПД, введении в эксплуатацию новых ИСПД, об изменении уровня защищенности существующих ИСПД, а также об инцидентах информационной безопасности, связанных с обработкой ПД в ИСПД.

8.5. В соответствии с Регламентом предоставления прав доступа и подключения автоматизированного рабочего места (далее – АРМ) к информационным ресурсам ИУС ПАО «Газпром» назначает приказом по Обществу ответственных администратора АРМ и администратора ИБ из числа работников ОИТТиС и ГКЗ соответственно.

9. Вывод ИСПД из эксплуатации

9.1. Решение о выводе ИСПД из эксплуатации принимает Функциональный заказчик (Владелец ИСПД).

9.2. Основаниями для вывода ИСПД из эксплуатации, в частности, могут быть:

- изменение требований законодательства Российской Федерации;
- изменение требований ПАО «Газпром»;
- изменение требований ООО «Газпром межрегионгаз»;
- распоряжения руководства Общества;
- предложения структурных подразделений.

9.3. Вывод ИСПД из эксплуатации осуществляется на основании приказа генерального директора Общества, подготовку которого организует Владелец ИСПД. Проект данного приказа согласовывается с ОИТТиС и ГКЗ.

9.4. В приказе о выводе ИСПД из эксплуатации указывается:

- наименование ИСПД;
- основания для вывода ИСПД из эксплуатации.

9.5. При выводе ИСПД из эксплуатации обеспечивается создание резервных копий (при необходимости и наличии правовых оснований) и гарантированное удаление ПД из запоминающих устройств.

9.6. По факту вывода ИСПД из эксплуатации оформляется акт (Приложение № 4), в котором должно быть отражено:

- наименование ИСПД, выводимой из эксплуатации;
- перечень действий, выполненных в ИСПД (резервное копирование информации, сведения о частичном либо полном уничтожении информации и др.);
- перечень изъятых машинных носителей ПД с информацией о факте уничтожения ПД, сроках и месте их хранения.

9.7. При выводе машинных носителей ПД из состава ИСПД, прекращении хранения на них ПД, содержащиеся ПД должны быть уничтожены способом, не допускающим возможности восстановления ПД, в порядке, установленном ЛНА Общества.

9.8. При выводе из эксплуатации машинного носителя ПД или содержащей такие носители ИСПД машинные носители ПД должны уничтожаться способом, не допускающим возможности восстановления содержащихся на них ПД, в порядке, установленном ЛНА Общества.

9.9. Факты уничтожения ПД и машинных носителей ПД отражаются в порядке, установленном ЛНА Общества.

9.10. При выводе из эксплуатации ИСПД, являющихся ЭСОД Общества, необходимо руководствоваться в том числе требованиями, установленными в Инструкции ЭСОД.

10.Права и обязанности

10.1. Владелец ИСПД

организует работы по созданию (модернизации) ИСПД;

организует работы по выводу из эксплуатации ИСПД;

контролирует соблюдение сроков и условий обработки ПД в ИСПД;

уничтожает или организует уничтожение (обезличивание) ПД в отношении которых: цель обработки достигнута; сроки обработки, указанные в согласии субъекта ПД, истекли; обработка должна быть прекращена в связи с отзывом субъекта ПД согласия на обработку его ПД, если иное не предусмотрено законодательством Российской Федерации, с оформлением соответствующих актов;

в целях контроля условий, определяющих необходимость модернизации ИСПД, осуществляет мониторинг изменения категорий ПД, обрабатываемых в ИСПД, и/или категорий и количества субъектов, ПД которых обрабатываются в ИСПД;

участвует в расследовании фактов несанкционированного доступа к ПД, обрабатываемых в ИСПД;

разрешает предоставление доступа пользователей к ИСПД;

учитывает используемые в структурном подразделении владельца ИСПД внешние носители ПД;

информирует ОКЗ о начале работ по созданию (модернизации) ИСПД, введении в эксплуатацию новых ИСПД, выводе из эксплуатации ИСПД, о возможной необходимости изменения уровня защищенности ПД, а также об инцидентах ИБ, связанных с обработкой ПД в ИСПД;

в порядке, установленном ЛНА Общества, представляет предложения по изменению соответствующих перечней должностей структурных подразделений Общества, замещение которых предусматривает осуществление обработки ПД.

10.2. Пользователи ИСПД

10.2.1. Работники, допущенные к обработке ПД в ИСПД (пользователи ИСПД), при выполнении возложенных на них функций должны исполнять требования по обеспечению информационной безопасности, установленные для работы в вычислительной сети (на автономном автоматизированном рабочем месте), в ИСПД, а также при использовании внешних носителей ПД.

10.2.2. Указанные в п. 10.2.1 работники при работе с ПД в ИСПД обеспечивают:

соблюдение конфиденциальности ПД (кроме общедоступных или обезличенных данных субъектов), в том числе исключение возможности несанкционированного ознакомления с содержанием ПД, хранящихся на используемых ими машинных носителях ПД, и (или) использования машинных носителей ПД в иных информационных системах;

информирование ОКЗ и ПСЭ об обнаружении попыток несанкционированного доступа к ИСПД (например, при невозможности входа в систему при использовании заведомо правильных логина и пароля, при пропаже (изменении) хранимой информации, наличии следов вскрытия аппаратных средств).

10.3. Руководитель структурного подразделения Общества

Руководители структурных подразделений Общества отвечают за выполнение в их структурных подразделениях требований Положения и обеспечивают:

контроль за соблюдением работниками требований Положения и требований к защите ПД, обрабатываемых в ИСПД;

размещение используемых в структурном подразделении устройств вывода (отображения) информации, исключающее несанкционированный просмотр ПД;

информируют ОКЗ об инцидентах информационной безопасности, связанных с обработкой ПД в ИСПД;

организуют учет внешних носителей ПД.

10.4. Отдел корпоративной защиты

10.4.1. Организация процесса обеспечения безопасности ПД, обрабатываемых в ИСПД, и контроль за эффективностью мер защиты ПД в ИСПД в Обществе возлагаются на ОКЗ.

10.4.2 ОКЗ:

осуществляет разработку ЛНА по вопросам обеспечения безопасности ПД, обрабатываемых в ИСПД;

принимает участие в согласовании требований к ИСПД в части СЗПД, модели угроз безопасности ПД, модели нарушителя безопасности ПД, акта определения уровня защищенности ПД, обрабатываемых в ИСПД;

принимает участие в согласовании проектной и эксплуатационной документации на ИСПД в части СЗПД;

принимает участие в проведении приемочных испытаний ИСПД в части СЗПД;

в случаях, предусмотренных правилами управления доступом к информационным системам Общества (в том числе ИСПД), принимает участие в согласовании заявок на доступ пользователей и администраторов к ИСПД, осуществляет контроль за тем, чтобы доступ к ПД, обрабатываемым в ИСПД, предоставлялся только работникам, должности которых включены в Перечень;

оказывает структурным подразделениям, участвующим в создании и эксплуатации СЗПД, методическую помощь по вопросам построения СЗПД и обеспечения безопасности ПД, обрабатываемых в ИСПД;

планирует и проводит проверки соблюдения требований законодательства Российской Федерации по обеспечению безопасности ПД, обрабатываемых в ИСПД, требований Положения и эффективности мер защиты ПД, реализованных в рамках СЗПД;

осуществляет мониторинг событий информационной безопасности в СЗПД (ИСПД);

участвует в обнаружении и организует расследование фактов несанкционированного доступа к ПД, обрабатываемым в ИСПД, а также других инцидентов, связанных с нарушением безопасности ПД;

ведет учет ИСПД, используемых в структурных подразделениях;

осуществляет контроль выполнения требований информационной безопасности в части защиты ПД при их обработке в ИСПД;

сопровождает проверки обеспечения безопасности ПД, обрабатываемых в ИСПД, проводимые уполномоченными федеральными органами исполнительной власти.

10.5. Структурное подразделение Общества, осуществляющее сопровождение эксплуатации ИСПД (ПСЭ)

10.5.1. Ответственность за внедрение и эксплуатацию ИСПД, входящих в ее состав средств защиты информации (или сопровождение перечисленных работ в случае привлечения к ним сторонних организаций), возлагается в Обществе на ПСЭ.

10.5.2. ПСЭ выполняет следующие функции:

проводит обследование ИСПД;

определяет актуальные угрозы безопасности ПД, обрабатываемых в ИСПД, и их тип, разрабатывают модель нарушителя безопасности ПД;

принимает участие в определении уровня защищенности ПД, обрабатываемых в ИСПД, и в проведении приемочных испытаний СЗПД;

подготавливает техническое задание на создание (модернизацию) ИСПД, перечень требований к СЗПД и состав мер по обеспечению безопасности ПД при их обработке в ИСПД, в том числе в соответствии с п. 4.7 Положения, согласовывает его с ОКЗ в части выполнения требований по защите ПД;

осуществляет выбор и внедрение организационно-технических мер, выполнение которых обеспечивает выполнение требований к защите ПД при их обработке в ИСПД для установленного уровня защищенности, а также нейтрализацию актуальных угроз безопасности ПД;

разрабатывает документы ИСПД, согласовывает их с Владельцем ИСПД и ГКЗ и утверждает в установленном в Обществе порядке;

согласовывает документы ИСПД, разрабатываемые юридическими лицами и индивидуальными предпринимателями, осуществляющими на договорной основе работы по созданию, модернизации ИСПД, внедрению и эксплуатации входящих в ее состав средств защиты информации;

обеспечивает хранение комплекта документации на ИСПД;

проводит резервное копирование ПД и восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним либо поврежденных вследствие иных причин;

учитывает используемые в ИСПД машинные носители ПД, в том числе используемые при обслуживании ИСПД внешние носители ПД;

реализует доступ работников к ПД, обрабатываемым в ИСПД, в строгом соответствии с полномочиями, определенными в соответствующих заявках, и ведет учет полномочий пользователей и администраторов ИСПД в матрице доступа;

хранит оригиналы исполненных заявок на допуск работников к ИСПД;

обнаруживает факты несанкционированного доступа к ПД, информирует об этом ГКЗ, принимает участие в расследовании таких фактов;

информирует ОКЗ об инцидентах информационной безопасности, связанных с обработкой ПД в ИСПД;

в случаях, установленных Положением, или по указанию Владельца ИСПД осуществляет удаление либо обезличивание ПД с оформлением соответствующих актов.

11.Обезличивание ПД

11.1. Обезличивание ПД, обрабатываемых в ИСПД, осуществляется в соответствии с Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, утвержденными приказом Роскомнадзора от 05 сентября 2013 г. № 996.

11.2. В состав проектной и эксплуатационной документации на ИСПД, в которой используются методы обезличивания ПД, должны включаться следующие материалы:

описание применяемых процедур обезличивания/деобезличивания ПД и их программного обеспечения;

правила (инструкции) по проведению процедур обезличивания/деобезличивания ПД;

правила (инструкции) по обработке обезличенных данных;

правила (инструкции) проведения контроля качества обезличенных данных и процедур обезличивания;

техническая и эксплуатационная документация, поставляемая с программными средствами обезличивания/деобезличивания ПД.

11.3. Информация, содержащая параметры методов и процедур обезличивания/деобезличивания ПД, относится к конфиденциальной информации ООО «Газпром межрегионгаз Тамбов».

12.Контроль за соблюдением требований ИБ

12.1. Проверки соблюдения требований законодательства Российской Федерации по обеспечению безопасности ПД, обрабатываемых в ИСПД, проводятся ОКЗ в рамках плановых проверок состояния обеспечения информационной безопасности в подразделениях Общества.

12.2. Оценка эффективности мер по обеспечению безопасности ПД, обрабатываемых в ИСПД, проводится не реже одного раза в 3 года в соответствии с п. 17 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119.

Начальник отдела
корпоративной защиты **А.В. Залевский**
« » 2025 г.