УТВЕРЖДЕНО
приказом ООО «Газпром межрегионгаз Север»
от 19.12.2022 № ТЮС-О/203/22

ПОЛИТИКА
обработки персональных данных в ООО «Газпром межрегионгаз Север» и управляемых организациях

Тюмень

Оглавление

1. Общие положения

1.1. Настоящая Политика обработки персональных данных в ООО «Газпром межрегионгаз Север» и управляемых организациях (далее - Политика) определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в ООО «Газпром Межрегионгаз Север» и управляемых организациях (далее - Общество) персональных данных, функции Общества при обработке персональных данных, права субъектов персональных данных, а также реализуемые в Обществе требования к защите персональных данных.

1.2. Политика разработана с учетом требований законодательных и иных нормативных правовых актов Российской Федерации в области обработки персональных данных.

1.3.Положения Политики служат основой для разработки организационно-распорядительных документов Общества, регламентирующих процессы обработки персональных данных, а также меры по обеспечению безопасности персональных данных при их обработке в Обществе.

2. Законодательная и нормативно-правовая база

Настоящая Политика определяется в соответствии со следующими нормативными правовыми актами:

2.1. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ.

2.2. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».

2.3. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».

2.4.Постановление Правительства Российской Федерации от 06.07.2008 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

2.5.Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2.6.Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.7. Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2.8.Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

2.9.Иные нормативные правовые акты органов государственной власти Российской Федерации.

3. Основные термины, понятия и определения

В настоящей Политике используются следующие основные термины, понятия и определения:

3.1. Информация - сведения (сообщения, данные) независимо от формы их представления.

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

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

3.4. 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.

3.5. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

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

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

3.8.Блокирование персональных данных – временное прекращение обработки персональныхданных (за исключением случаев, если обработка необходима для уточнения персональных данных).

3.9. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

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

4. Принципы и цели обработки персональных данных

4.1. Общество, являясь операторами персональных данных, осуществляет обработку персональных данных работников Общества и иных субъектов

персональных данных, не состоящих с Обществом в трудовых отношениях.

4.2. Обработка персональных данных в Обществе осуществляется с учетом необходимости обеспечения защиты прав и свобод работников Общества и иных субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

обработка персональных данных осуществляется в Обществе на законной и справедливой основе;

обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

обработке подлежат только персональные данные, которые отвечают целям их обработки;

содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;

при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Общества принимают необходимые меры либо обеспечивают их принятие по удалению или уточнению не полных или неточных персональных данных;

обрабатываемые персональные данные уничтожаются либо обезличиваются по достижению целей обработки или в случае утраты необходимости достижения этих целей, если иное не предусмотрено законодательством Российской Федерации.

4.3. Персональные данные в Обществе обрабатываются в целях: обеспечения соблюдения требований Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов ООО «Газпром межрегионгаз» и Общества;

осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Общество, в том числе по предоставлению персональных данных в органы государственной власти (Федеральная налоговая служба, Пенсионный фонд Российской Федерации, Федеральный фонд обязательного медицинского страхования, а также иные органы государственной власти);

регулирования трудовых отношений с работниками Общества (содействие в трудоустройстве, обучение и продвижение по службе, обеспечение личной безопасности, контроль количества и качества выполняемых работ, обеспечение сохранности имущества);

предоставления работникам Общества и членам их семей дополнительных гарантий и компенсаций, в том числе негосударственного пенсионного обеспечения, добровольного медицинского страхования, медицинского обслуживания и других видов социального обеспечения;

защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;

подготовки, заключения, исполнения и прекращения договоров с

контрагентами;

обеспечения пропускного и внутриобъектового режимов на объектах Общества;

формирования справочных материалов для внутреннего информационного обеспечения деятельности группы лиц ПАО «Газпром»;

исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации;

осуществления прав и законных интересов Общества в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Общества или третьих лиц, либо достижение общественно значимых целей;

в иных законных целях.

5. Перечень субъектов, персональные данные которых обрабатываются в Обществе.

В Обществе в зависимости от задач и функций, возложенных на Структурные подразделения, обрабатываются персональные данные следующих категорий субъектов персональных данных:

- Работники Общества;
- Кандидаты на замещение вакантных должностей в Обществе, включая его филиалы и управляемые организации;
- Пенсионеры Общества;
- Работники филиалов и управляемых организаций Общества;
- Кандидаты на замещение вакантных должностей в филиалах и управляемых организациях Общества;
- Члены семей и близкие родственники работников Общества;
- Лица, имеющие право на социальное обеспечение в соответствии с коллективными договорами и локальными нормативными актами Общества;
- Лица, наделенные правом подписи от имени Общества (договоров, контрактов, соглашений, актов и т.д.);
- Кандидаты для избрания в органы управления и контроля объектов вложений Общества и члены указанных органов;
- Члены семей работников или пенсионеров Общества (по договорам добровольного медицинского страхования);
- Контрагенты Общества (физические лица);
- Физические лица в цепочке собственников контрагентов Общества;
- Акционеры и бенефициары Общества;
- Инсайдеры Общества;
- Представители организаций, участвующих в третейских разбирательствах;
- Физические лица, направляющие обращения в Общество;
- Иные субъекты персональных данных (для обеспечения реализации целей обработки, указанных в разделе 4 настоящей Политики).

6. Перечень персональных данных, обрабатываемых в Обществе

6.1. Перечень персональных данных (Приложение 1), обрабатываемых в Обществе, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Общества с учетом целей обработки персональных данных, указанных в разделе 4 настоящей Политики.

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

7. Функции Общества при осуществлении обработки персональных данных

Общество при осуществлении обработки персональных данных выполняет следующие функции:

7.1. Принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов Общества в области обработки персональных данных.

7.2. Принимает правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также иных неправомерных действий в отношении персональных данных.

7.3.Назначает лицо, ответственное за организацию обработки персональных данных в Обществе.

7.4.Издаёт локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных в Обществе.

7.5.Осуществляет ознакомление работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локальных нормативных актов Общества в области обработки персональных данных, в том числе с требованиями к защите персональных данных, и обучение указанных работников.

7.6. Публикует настоящую Политику на Интернет-сайте Общества и обеспечивает неограниченный доступ к ней.

7.7.Сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации.

7.8.Прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации.

7.9.Совершает иные действия, предусмотренные законодательством Российской Федерации в области обработки персональных данных.

8. Условия обработки персональных данных в Обществе

8.1.Обработка персональных данных в Обществе осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации.

8.2. Без согласия субъекта персональных данных Общество не передаёт третьим лицам и не распространяет его персональные данные, если иное не предусмотрено законодательством Российской Федерации.

8.3. Общество вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

8.4. В целях внутреннего информационного обеспечения деятельности группы лиц ПАО «Газпром» могут создаваться внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, место работы, должность, год и место рождения, адрес, абонентский номер, адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.

8.5 Доступ к обрабатываемым в Обществе персональным данным разрешается только работникам Общества, занимающими должности, включенные на основании приказа Общества в перечень должностей структурных подразделений Общества, при замещении которых осуществляется обработка персональных данных.

9. Перечень действий с персональными данными и способы их обработки

9.1. Общество осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

9.2. Обработка персональных данных в Обществе осуществляется следующими способами:

неавтоматизированная обработка персональных данных;

автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;

смешанная обработка персональных данных.

10. Права субъектов персональных данных

Субъекты персональных данных имеют право на:

10.1. Полную информацию об их персональных данных, обрабатываемых в Обществе.

10.2. Доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренным законодательством Российской Федерации.

10.3. Уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми

для заявленной цели обработки.

10.4. Отзыв согласия на обработку персональных данных.

10.5. Принятие предусмотренных законодательством Российской Федерации мер по защите своих прав.

10.6. Обжалование действия или бездействия Общества, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или суд.

10.7. Осуществление иных прав, предусмотренных законодательством Российской Федерации.

11. Меры, принимаемые Обществом для обеспечения выполнения обязанностей оператора при обработке персональных данных

11.1.Меры, необходимые и достаточные для обеспечения выполнения Обществом обязанностей оператора, предусмотренных законодательством Российской Федерации в области обработки персональных данных, включают:

назначение лица, ответственного за организацию обработки персональных данных в Обществе;

принятие локальных нормативных актов и иных документов в области обработки и защиты персональных данных;

организацию обучения и проведение методической работы с работниками Общества, занимающими должности, включенные на основании приказа Общества в перечень должностей структурных подразделений Общества, при замещении которых осуществляется обработка персональных данных;

получение согласий субъектов персональных данных на обработку персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;

обособление персональных данных, обрабатываемых без использования средств автоматизации, от иной информации, в частности, путем их фиксации на отдельных материальных носителях персональных данных, в специальных разделах;

обеспечение раздельного хранения персональных данных и их материальных носителей, обработка которых осуществляется в разных целях и которые содержат разные категории персональных данных;

установление запрета на передачу персональных данных по открытым каналам связи, вычислительным сетям вне пределов контролируемой зоны, Единой ведомственной сети передачи данных (ЕВСПД) ПАО «Газпром» и сети Интернет без применения установленных в Обществе мер по обеспечению безопасности персональных данных (за исключение общедоступных и (или) обезличенных персональных данных);

хранение материальных носителей персональных данных с соблюдением условий, обеспечивающих их сохранность и исключающих несанкционированный доступ к ним;

осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам Общества;

иные меры, предусмотренные законодательством Российской Федерации в области обработки персональных данных.

11.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с требованиями законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Общества, регламентирующих вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Общества.

11.3. Лицо, ответственное за организацию обработки персональных данных и назначаемое приказом Общества, получает указания от руководства Общества и подотчетно ему.

11.4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано организовывать:

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

доведение до сведения работников Общества положений законодательства Российской Федерации, локальных нормативных актов Общества в области обработки персональных данных, в том числе требований к защите персональных данных;

контроль за приемом и обработкой обращений и запросов субъектов персональных данных или их представителей.

12. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Обществ в области обработки персональных данных, в том числе требований к защите персональных данных

12.1. Контроль за соблюдением структурными подразделениями Общества законодательства Российской Федерации, локальных нормативных актов Общества в области обработки персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных в Обществе законодательству Российской Федерации, локальным нормативным актам Общества в области обработки персональных данных, в том числе требованиям к защите персональных данных, а также принятых мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области обработки персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.

12.2. Внутренний контроль за соблюдением структурными подразделениями Общества законодательства Российской Федерации, локальных нормативных актов Общества в области обработки персональных данных, в том числе требований к защите персональных данных, осуществляет Заместителем генерального директора по корпоративной защите ООО «Газпром Межрегионгаз Север».

12.3.Персональная ответственность за соблюдение структурными подразделениями Общества требований законодательства Российской Федерации, локальных нормативных Общества в области обработки персональных данных, в том числе требований к защите персональных данных, возлагается на начальников структурных подразделений Общества.

Приложение № 1
к Политике обработки персональных данных

ПЕРЕЧЕНЬ
персональных данных, подлежащих защите в информационных системах персональных данных ООО "Газпром межрегионгаз Север" и управляемых организаций

1. Общие положения

Настоящий Перечень персональных данных, подлежащих защите в информационных системах персональных данных ООО "Газпром межрегионгаз Север" и управляемых организаций (далее – Перечень), разработан в соответствии со следующими документами:

Трудовым кодексом Российской Федерации от 30 декабря 2001 г. № 197-ФЗ, Гражданским кодексом Российской Федерации;

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;

Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687;

требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, утвержденными постановлением Правительства Российской Федерации от 06 июля 2008 г. № 512;

требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119;

иными нормативными правовыми актами Российской Федерации и локальными нормативными актами ООО «Газпром межрегионгаз Север», регламентирующими вопросы обработки персональных данных и иной конфиденциальной информации.

Федеральным законом от 26 июля 2006 г. № 152 «О персональных данных» и нормативно-правовыми актами ООО «Газпром межрегионгаз».

Перечень содержит полный список категорий данных, безопасность которых обеспечивается системой защиты персональных данных (СЗПДн).

2. Персональные данные, обрабатываемые в информационных системах персональных данных

2.1. В информационных системах персональных данных ООО «Газпром межрегионгаз Север» и управляемых организаций (далее – ИСПДн) обрабатываются персональные данные следующих категорий субъектов ПДн:

работники Общества;

бывшие работники Общества, трудовые отношения с которыми прекращены;

кандидаты на замещение вакантных должностей в Обществе;

пенсионеры Общества;

работники управляемых организаций Общества;

кандидаты на замещение вакантных должностей в управляемых организациях Общества;

члены семей и близкие родственники работников Общества, его филиалов и управляемых организаций;

лица, имеющие право на социальное обеспечение в соответствии с коллективными договорами и локальными нормативными актами Общества;

лица, наделенные правом подписи от имени Общества (договоров, контрактов, соглашений, актов и т.д.);

кандидаты для избрания в органы управления и контроля объектов вложений Общества и члены указанных органов;

члены семей работников или пенсионеров Общества (по договорам добровольного медицинского страхования);

посетители, пропускаемые на объекты Общества;

контрагенты Общества, его филиалов и управляемых организаций (физические лица);

физические лица в цепочке собственников контрагентов Общества;

акционеры и бенефициары Общества;

инсайдеры Общества;

физические лица, направляющие обращения в Общество, его филиалы и управляемые организации;

другие субъекты персональных данных, перечисленные в Регламентах.

2.2. Обработка персональных данных осуществляется в целях исполнения заявок (на получение технических условий, на проведение проектно-изыскательских работ, на заключение договора технического присоединения, на проведение строительно-монтажных работ, на проведение пуско-наладочных работ), исполнения гражданско-правовых договоров, осуществления взаимодействия при ответе на обращения, исполнения требований нормативно-правовых актов, регламентирующих взаимодействие с органами власти, органами публичной власти Тюменской области, ХМАО, ЯНАО, при реализации мероприятий межрегиональных и региональных программ газификации жилищно-коммунального хозяйства, промышленных и иных организаций, обеспечения соблюдения законов и иных нормативных правовых актов, локальных нормативных актов ООО «Газпром межрегионгаз Север», обеспечения задач кадровой работы, в том числе кадрового учета, делопроизводства, содействия в осуществлении служебной (трудовой) деятельности, обеспечения и продвижения по работе, формирования кадрового резерва, обучения и

должностного роста, учета результатов исполнения должностных обязанностей, обеспечения личной безопасности субъектов персональных данных, обеспечения сохранности имущества, обеспечения установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, формирования внутренних справочных материалов, содержащих персональные данные, и определения общедоступных персональных данных, а также в целях противодействия коррупции.

2.3. Персональные данные обрабатываются в ИСПДн ООО «Газпром межрегионгаз Север» и управляемых организаций до момента достижения целей обработки персональных данных.

Приложение № 2
к Политике обработки персональных данных

ПОЛОЖЕНИЕ
о контролируемой зоне ООО "Газпром межрегионгаз Север" и управляемых организаций

1. Общие положения

1.1. Настоящая Инструкция о контролируемой зоне ООО "Газпром межрегионгаз Север" и управляемых организаций (далее – Инструкция) разработана в соответствии с приказом ФСТЭК от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Политикой физической защиты информации, утвержденной приказом от 11.08.2015 №ГМС-О/98/15, Регламентом физической защиты информации, утвержденным приказом от 31.01.2017 №ГМС-О/15/17. Инструкция разработана с целью определения границы контролируемой зоны для обеспечения физической охраны ИСПДн, создания контроля доступа в помещения посторонних лиц и предотвращения несанкционированного проникновения в помещения информационной системы и хранилище носителей информации.

2. Ограничение доступа к средствам ИСПДн

2.1. В целях надежного обеспечения физической охраны технические средства обработки персональных данных ИСПДн должны располагаться только в помещениях, находящихся в зоне ответственности работников охранного предприятия.

2.2. Ограничение входа на территорию, где находятся технические средства обработки персональных данных ИСПДн, осуществляется путем контроля со стороны работников охранного предприятия и установки турникетов и дверей со специальными устройствами контроля доступа.

2.3. Выдача электронных карт допуска осуществляется отделом инженерно-технических средств защиты по заявке на предоставление доступа, согласованной администратором ИБ.

2.4. Двери помещений, в которых установлены средства обработки персональных данных ИСПДн, должны быть оборудованы запирающими устройствами (замками). Ключи от помещений, относятся к предметам строгой отчетности и выдаются только лицам, работающим в данном помещении, под роспись в журнале учета ключей от режимных помещений.

2.5. Работник, получивший электронную карту допуска и ключи, обеспечивает их сохранность. Передача электронной карты допуска и ключа посторонним лицам, оставление их без присмотра, а также изготовление их дубликатов запрещается.

2.6. В случае утраты ключа от режимного помещения либо электронной карты допуска, работник через непосредственного руководителя немедленно докладывает служебной запиской с объяснением обстоятельств утраты

начальнику отдела инженерно-технических средств защиты. По каждому случаю утраты назначается служебная проверка.

3. Охрана помещений ИСПДн

3.1. По окончании рабочего времени, помещения, в которых находятся средства обработки персональных данных, должны сдаваться под охрану работникам охранного предприятия, путем записи в специальном журнале. Перед вскрытием помещения работник, осуществляющий вскрытие, обязан произвести запись в журнале, указав свои данные и время вскрытия.

3.2. В соответствии с планом охраны работники охранного предприятия осуществляют обход здания, проверяя целостность дверей, замковых устройств. При внешнем осмотре прилегающей территории к административному зданию обращается внимание также на целостность окон, их закрытие, не выключенное освещение в помещениях.

3.3. Обо всех случаях нарушения установленного порядка сдачи (вскрытия) помещений сотрудники охранного предприятия обязаны письменно докладывать начальнику отдела инженерно-технических средств защиты.

Приложение № 3
к Политике обработки персональных данных

ИНСТРУКЦИЯ
по учету лиц, допущенных к работе с персональными данными

1. Общие положения

1.2.Настоящая Инструкция по учету лиц, допущенных к работе с персональными данными (далее – Инструкция), разработана в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

1.3.Инструкция разработана с целью организации учета лиц, допущенных к работе с персональными данными в ИСПДн ООО "Газпром межрегионгаз Север" и управляемых организаций.

2. Порядок допуска к работе с персональными данными

2.4.Основанием для допуска к работе с персональными данными, обрабатываемыми в ИСПДн, является должностная инструкция и включение в Список работников, осуществляющих обработку персональных данных в Структурном подразделении.

2.5. Прекращением допуска к работе с персональными данными, обрабатываемыми в ИСПДн, служит приказ об увольнении или переводе работника на должность. не связанную с обработкой персональных данных, либо исключение работника из Списка работников, осуществляющих обработку персональных данных в Структурном подразделении.

2.6. При выявлении нарушений требований руководящих документов по соблюдению требований безопасности персональных данных, доступ лиц, допустивших нарушения, к работе с персональными данными приостанавливается до окончания служебной проверки.

3. Учет лиц, допущенных к работе с персональными данными

3.1. Учет, допущенных к работе с персональными данными в ИСПДн, производится в Журнале учета лиц, допущенных к работе с персональными данными в ИСПДн ООО "Газпром межрегионгаз Север" и управляемых организаций (далее – Журнал).

3.2. Журнал ведется администратором ИСПДн.

3.3. Ведение журнала осуществляется в электронном виде.

3.4. На бумажном носителе Журнал ведется до его полного заполнения. Заполненные журналы хранятся не менее 3 лет после их полного заполнения.

3.5. Все запросы пользователей ИСПДн на получение персональных данных и факты предоставления персональных данных по этим запросам должны регистрироваться автоматизированными средствами информационной системы в электронном журнале обращений, содержание которого должно периодически проверяться администратором информационной безопасности.

ФОРМА
журнала учета лиц, допущенных к работе с персональными данными в информационных системах

Фамилия Имя Отчество

№ п/п	Сведения о допуске к персональным данным				Сведения о прекращении допуска к персональным данным		
	Наименование ИСПДн	Полномочия в ИСПДн (чтение, запись, изменение, администрирование)	№ заявки и дата утверждения, внесения изменений в «Список работников, осуществляющих обработку ПД»	Дата и подпись допускаемого лица	№ приказа и дата утверждения «Список работников, осуществляющих обработку ПД»	Номер и дата приказа об увольнении, переводе на другую должность	Дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн

Приложение № 4
к Политике обработки персональных данных

ИНСТРУКЦИЯ
о порядке учета, хранения и уничтожения носителей персональных данных

1. Общие положения

1.1. Настоящая Инструкция о порядке учета, хранения и уничтожения носителей персональных данных информационной системы персональных данных ООО «Газпром межрегионгаз Север» и управляемых организаций (далее - Инструкция) разработана в соответствии с Федеральными законами от 27.07.2006 № 152 «О персональных данных» и 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», приказом ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Регламентом использования мобильных программно-технических устройств и съемных носителей информации, утвержденного приказом от 31.01.2017 №ГМС-О/15/17.

1.2.Инструкция устанавливает порядок использования, хранения и уничтожения носителей персональных данных (далее – носитель ПДн), используемых в ИСПДн ООО "Газпром межрегионгаз Север" и управляемых организаций.

1.3.Под носителем ПДн понимается любой материальный (бланк, книгу, реестр и т.д.), машиночитаемый магнитный, оптический или электронный носитель информации, способный достаточно длительное время сохранять в своей структуре занесенную в него информацию, на который произведена запись с персональными данными физических лиц.

1.4.Носители ПДн подразделяются на носители многократной и однократной записи. Носители ПДн многократной записи позволяют многократно записывать, воспроизводить и стирать информацию. Носители однократной записи позволяют однократно записать информацию и многократно ее считывать.

1.5. Кроме того, носители ПДн разделяются на съемные и стационарные. Стационарные носители ПДн – носители информации многократной записи, установленные на автоматизированные рабочие места и серверные станции ИСПДн, и предназначенные для обработки и хранения персональных данных. Съемные носители ПДн – носители информации многократной либо однократной записи и предназначенные для хранения, либо транспортировки персональных данных.

2. Порядок учета носителей ПДн

2.1. Под использованием электронных носителей ПДн понимается их подключение к ИСПДн с целью обработки и хранения занесенной в них информации.

2.2. Под использованием материальных носителей ПДн понимается их заполнение без использования средств автоматизации с целью обработки и хранения занесенной в них информации.

2.3. Учет стационарных электронных носителей ПДн осуществляет ответственными работниками отдела информационных технологий и связи. Факт установки носителей ПДн в ИСПДн фиксируется в журнале учета носителей ПДн (Приложение 1).

2.4. Учет и выдачу съемных электронных носителей ПДн осуществляет в соответствии с Инструкцией по конфиденциальному делопроизводству.

2.5. Съемный носитель ПДн выдается пользователю для выполнения работ на конкретный срок. По окончании работ пользователь обязан сдать носитель ПДн администратору ИБ.

2.6. При использовании пользователями съемных носителей ПДн необходимо соблюдать следующие требования:

- бережно относится к носителям конфиденциальной информации;
- использовать носители ПДн исключительно для выполнения своих служебных обязанностей;
- обеспечивать физическую безопасность носителей информации всеми разумными способами;
- извещать администратора ИБ о фактах утраты (кражи) носителей ПДн и ставить в известность о любых фактах нарушения требований настоящей Инструкции.

2.7. При использовании съемных носителей ПДн запрещено:

- использовать их в личных целях;
- передавать другим лицам, за исключением администратора ИБ;
- хранить их вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить из служебных помещений для работы с ними на дому и т. д.

2.8. При выводе автоматизированного рабочего места (АРМ), либо серверной станции из состава ИСПДн, установленные в них стационарные носители ПДн (жесткие диски) подлежат снятию и помещению на хранение, либо уничтожению. Снятый носитель ПДн в дальнейшем может быть установлен на другое АРМ или серверную станцию входящие в состав ИСПДн. Информация о снятии носителя ПДн с одного АРМ или серверной станции и установки на другие обязательно регистрируется в журнале учета носителей персональных данных.

2.9. В случае утраты, порчи носителей ПДн, либо разглашении содержащихся в них сведений, немедленно ставится в известность администратор ИБ.

2.10. Все носители ПДн являются собственностью ООО "Газпром межрегионгаз Север" и управляемых организаций и подвергаются регулярной ревизии и контролю. Ревизия носителей ПДн, хранящихся у ответственного лица, выданных пользователям и установленных на АРМ и серверные станции проводится не реже одного раза в год.

2.11.По факту утраты, порчи либо несанкционированного или нецелевого использовании носителей ПДн инициализируется служебная проверка.

3. Порядок хранения носителей ПДн

3.1. В целях поддержания непрерывности работы и восстановления работоспособности ИСПДн, а также для минимизации последствий внештатных и аварийных ситуаций в работе ИСПДн применяется резервное копирование персональных данных.

3.2. Порядок резервного копирования персональных данных определен Инструкцией о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в ООО "Газпром межрегионгаз Север" и управляемых организациях.

3.3. Носители, на которые произведено резервное копирование персональных данных, а также другие неиспользуемые носители ПДн подлежат обязательному учету.

3.4. Шкафы, предназначенные для хранения носителей ПДн, должны располагаться в специальных помещениях и защищать носители ПДн от механических повреждений и деформаций, загрязнения и запыления, воздействия электромагнитных полей, экстремальных температур и прямых солнечных лучей.

3.5. Оптимальным режимом хранения для электронных носителей информации является температура в помещении +23° - +25° С и относительная влажность 50%.

4. Порядок уничтожения носителей ПДн

4.1. Носители ПДн, выслужившие свой срок либо пришедшие в негодность, а также резервные носители ПДн, по окончании срока хранения подлежат уничтожению.

4.2. Уничтожение носителей ПДн производится в присутствии членов специально созданной комиссии, с обязательным составлением акта. В акт вносится марка, модель и серийный номер уничтожаемого носителя ПДн.

4.3. Уничтожение носителей ПДн производится путем физического воздействии на рабочие слои дисков, в результате которого разрушается физическая, магнитная или химическая структура рабочего слоя носителя ПДн.

4.4. В исключительных случаях, когда носитель ПДн предполагается использовать вне ИСПДн, уничтожается только находящаяся на нем информация с персональными данными. Уничтожение персональных данных производится при помощи специальных программ или программно-аппаратных комплексов путем многократной перезаписи в секторах магнитного диска.

4.5. В Журнале учета носителей персональных данных делается отметка об уничтожении носителя ПДн либо выводе его из состава ИСПДн.

Типовая форма
журнала учета съемных носителей конфиденциальной информации (персональных данных)

№ п/п	Тип/ёмкость машинного носителя персональных данных	Марка, модель и серийный, заводской, учетный или регистрационный номер	Место установки (регистрационный и инвентарный номер системного блока или сервера) либо должность, фамилия и инициалы лица которому выдан носитель, дата установки, выдачи	Расписка ответственного лица в установке, получении (подпись, ФИО, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Сведения об уничтожении машинных носителей персональных данных, стирании информации (номер и дата акта)
1						
2						
3						
…						
N						

А К Т №

уничтожения носителей персональных данных информационных систем персональных данных ООО "Газпром межрегионгаз Север" и управляемых организаций

_____ « ____ » _____ 20___ г
Место уничтожения Дата уничтожения

Комиссия, в составе:

_____

_____
(должности, фамилии и инициалы членов комиссии)

_____

_____

составили настоящий акт в том, что «____»_____20____ г. произведено уничтожение следующих носителей персональных данных информационной системы персональных данных ООО "Газпром межрегионгаз Север" и управляемых организаций,

_____
(марка, модель и серийный, заводской или учетный номер носителей информации)

_____

_____

Уничтожение произведено в нашем присутствии путем

_____
(указывается способ уничтожения носителей персональных данных)

Подписи членов комиссии:

_____ _____
(подпись) (Ф. И. О.)

_____ _____
(подпись) (Ф. И. О.)

А К Т №

уничтожения персональных данных с носителя персональных данных информационных систем персональных данных ООО "Газпром межрегионгаз Север" и управляемых организаций

_____ « _____ » _____ 20___ г

Место уничтожения — Дата уничтожения

Комиссия, в составе: _____

_____

(должности, фамилии и инициалы членов комиссии)

_____

_____

составили настоящий акт в том, что «____»_____20____ г. произведено уничтожение персональных данных с носителя персональных данных информационной системы персональных данных ООО "Газпром межрегионгаз Север" и управляемых организаций,

_____

_____

(марка, модель и серийный, заводской или учетный номер носителя информации)

_____

Уничтожение произведено в нашем присутствии путем _____

_____

(указывается способ уничтожения персональных данных)

Подписи членов комиссии:

_____ _____

(подпись) (Ф. И. О.)

_____ _____

(подпись) (Ф. И. О.)

Приложение № 5
к Политике обработки персональных данных

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных ООО "Газпром межрегионгаз Север" и управляемых организаций

1. Общие положения

1.4. Инструкция пользователя ИСПДн ООО "Газпром межрегионгаз Север" и управляемых организаций (далее – Инструкция) включает основные обязанности, права и ответственность пользователей, допущенных к автоматизированной обработке персональных данных и иной конфиденциальной информации в ИСПДн ООО "Газпром межрегионгаз Север" и управляемых организаций.

1.5. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

1.6. Пользователем является любой сотрудник ООО "Газпром межрегионгаз Север", его филиала и управляемых организаций, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, персональным данным и средствам защиты ИСПДн.

1.7. Для работы с персональными данными пользователь должен иметь навыки работы на ПЭВМ и быть допущен к обработке соответствующих категорий персональных данных.

1.8. Пользователь в своей работе руководствуется федеральными законами, постановлениями Правительства Российской Федерации, локальными нормативными документами Общества, регламентирующими обеспечение безопасности персональных данных, а также настоящей Инструкцией.

1.9. Методическое руководство работой пользователей ИСПДн осуществляется администратором ИБ.

2. Порядок обеспечения безопасности персональных данных

2.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

2.2. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

2.3. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а

также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

2.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, сформированными в соответствии с Регламентом управления доступом пользователей в Обществе. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

2.5. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

2.6. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;
- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

2.7. При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

3. Обязанности пользователя

3.1. Пользователь при обработке информации в ИСПДн в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных и несет персональную ответственность за соблюдение требований настоящей Инструкции и руководящих документов по защите информации.

3.2. Пользователь обязан:

- знать и выполнять требования действующих нормативных и руководящих документов Общества по обеспечению безопасности персональных данных;

- знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации;

- помнить личные пароли, не записывать их на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

- в случае необходимости хранения своих паролей на бумажном носителе, не оставлять их без присмотра и хранить только в личном, опечатанном сейфе, либо, в опечатанном личной печатью конверте, в сейфе у администратора ИСПДн или Администратора ИБ;

- получив личный пароль, запомнить его, и не при каких обстоятельствах не сообщать его другим лицам и не регистрировать их в системе под своим паролем;

- при работе с персональными данными, а также при вводе пароля, не допускать присутствия в помещении, где расположены средства вычислительной техники, лиц, не допущенных к обрабатываемой информации, и располагать экран видеомонитора так, чтобы исключалась возможность просмотра отображаемой на нем информации посторонними лицами и техническими средствами;

- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;

- соблюдать правила работы в сетях общего доступа и международного обмена – Интернет;

- знать штатные режимы работы программного обеспечения и способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, пути проникновения и распространения компьютерных вирусов;

- знать и соблюдать требования Регламента защиты от вредоносного ПО в информационной системе персональных данных Общества в пределах своих полномочий;

- в случае обнаружения зараженных компьютерными вирусами файлов пользователи приостановить работу, немедленно поставить в известность руководителя своего подразделения, администратора ИСПДн, администратора ИБ и владельца зараженных файлов.

3.3. Обо всех выявленных нарушениях, связанных с информационной безопасностью Общества, фактах или попытках несанкционированного доступа к обрабатываемой информации, а также для получений консультаций по вопросам обработки информации, настройки элементов ИСПДн и информационной безопасности обращаться к администратору ИСПДн или администратору ИБ.

4. Запрещаемые действия пользователя

Пользователю, обрабатывающему персональные данные средствами автоматизированных информационных систем, запрещается:

- самостоятельно подключать к АРМ (автоматизированному рабочему месту) какие-либо устройства и вносить изменения в состав или конфигурацию АРМ;

- самостоятельно устанавливать либо допускать к установке программных средств посторонних лиц (установка программного обеспечения осуществляется только специалистом отдела информационных технологий и связи);

- записывать и хранить персональные данные на неучтенных установленным порядком съемных носителях информации;

- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, а также на АРМ не входящих в состав ИСПДн;

- сообщать кому-либо устно или письменно личные пароли доступа к ресурсам АРМ и ИСПДн;

- отключать либо блокировать средства антивирусного контроля и средства защиты информации;

- оставлять бесконтрольно АРМ с загруженными персональными данными, с установленными маркированными сменными носителями, электронными ключами;

- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.

5. Права пользователя

Пользователь, в обязанности которого входит обработка персональных данных в ИСПДн, имеет право:

- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;

- обращаться к сотрудникам отдела информационных технологий и связи, администратору ИСПДн и ответственному за организацию работ по обеспечению безопасности персональных данных и другой конфиденциальной информации с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, а также со средствами защиты информации.

6. Ответственность

Пользователи ИСПДн несут персональную ответственность:

- за ненадлежащее выполнение требований настоящей инструкции;

- за соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по безопасности персональных данных, конфиденциальной информации, использование информационных ресурсов и средств защиты информации;

- за сохранность и работоспособность средств вычислительной техники.

6.1. За нарушение правил хранения и использования персональных данных, повлекшее за собой ущерб работнику или работодателю, сотрудник может быть привлечен к дисциплинарной и материальной ответственности в соответствии со ст.90 ТК РФ.

6.2. За нарушение порядка сбора, хранения, использования или распространения персональных данных сотрудник может быть привлечен к административной ответственности по ст. 13.11 КоАП РФ.

6.3. За нарушение неприкосновенности частной жизни, а именно разглашение сведений о частной жизни граждан, являющихся работниками или

абонентами ООО "Газпром межрегионгаз Север" и управляемых организаций, сотрудник может быть привлечен к уголовной ответственности по ст. 137 УК РФ.

6.4. За неправомерный доступ к охраняемой законом компьютерной информации (персональные данные и конфиденциальная информация) сотрудник может быть привлечен к уголовной ответственности по ст. 272 УК РФ.

6.5. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями и регламентами работы.

Приложение № 6
к Политике обработки персональных данных

Порядок обнаружения и реагирования на инциденты информационной безопасности

1. Общие положения

1.1. Настоящий Порядок разработан в соответствии с требованиями Политики информационной безопасности, утвержденной приказом ЗАО «Газпром межрегионгаз Север» от 08.08.2014 №ГМС-О/127/14 и Положением о порядке проведения служебного расследования в отношении работников ООО «Газпром межрегионгаз Север» и управляемых организаций, утвержденным приказом от 30.08.2018 №ГМС-О/189/18. Порядок рассматривает вопросы обнаружения, реагирования и расследование инцидентов информационной безопасности (далее - ИБ) в Обществе и управляемых организациях.

1.2. Порядок обязателен для применения во всех управляемых организациях и территориальных подразделениях Общества.

1.3. Настоящий Порядок при необходимости должен пересматриваться (актуализироваться) после каждого инцидента ИБ.

1.4. Организацию работ по реагированию на инцидент, его локализацию, ликвидацию (минимизацию) ущерба, выполняет заместитель генерального директора по корпоративной защите или председатель комиссии по защите информации (далее – комиссия по ЗИ) Общества.

1.5. Непосредственные работы по выявлению, реагированию, ликвидации и выработке мер для исключения проявления инцидента ИБ в дальнейшем проводит администратор информационной безопасности (далее – администратор ИБ) и сформированная группа реагирования на инцидент ИБ (далее - ГРИБ). В случае необходимости, для оказания помощи в рамках реагирования и расследования инцидента ИБ, администратор ИБ может привлекать любого сотрудника Общества и управляемых организаций.

2. Понятие инцидента информационной безопасности

Инцидентом ИБ называется нежелательное или неожиданное событие в системе защиты информации, которое имеет определенный шанс подвергнуть риску информационные ресурсы, вызвать сбой в работе оборудования, а также поставить под угрозу саму систему защиты информации. Инцидентом ИБ, в общем случае, называется любое нарушение политик ИБ Общества.

Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Инциденты ИБ преследуют нарушение одного или сразу нескольких основополагающих свойств информации:

- нарушение конфиденциальности;
- нарушение целостности;
- нарушение доступности.

Инциденты ИБ могут преследовать нарушение дополнительных (производных) свойств информации:

- нарушение надежности;
- нарушение достоверности;
- нарушение принципа неотрекаемости.

Все действия в процессе реагирования на Инцидент должны документироваться администратором ИБ в «Журнале учета инцидентов информационной безопасности».

Журнал ведется на бумажном носителе или в электронной форме. В случае если журнал ведется на бумажном носителе, он должен быть пронумерован и прошнурован, иметь пометку «конфиденциально» и учитываться по номенклатуре дел.

В кратчайшие сроки, не превышающие одного рабочего дня, администратор ИБ и администратор ИСПДн, предпринимают меры по восстановлению работоспособности ИСПДн. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

3. Обнаружение инцидентов

3.1. Информация об инцидентах ИБ может поступать по следующим каналам:

- информация, получаемая от сотрудников Общества и управляемых организаций по любым каналам связи: телефон, электронная почта, СЭД АСДОБ, служебная записка;
- журналы регистрации сетевого оборудования и межсетевых экранов;
- журналы регистрации общесистемного программного обеспечения;
- журналы регистрации прикладного программного обеспечения;
- оповещения антивирусных подсистем;
- оповещения подсистем обнаружения атак;
- оповещения других подсистем.

3.2. Сотрудники отдела информационных технологий, телекоммуникации и связи, осуществляющие техническую поддержку программного обеспечения и систем, обязаны при получении информации обо всех нетипичных событиях, относящихся к ИБ, незамедлительно сообщить о происходящем администратору ИБ.

3.3. Сотрудники Общества и управляемых организаций, работающие с информационными системами, при получении информации обо всех нетипичных событиях, сообщений системы, сообщений систем защиты (например, Антивирусной системы), обязаны незамедлительно сообщить о происходящем администратору ИБ или сотруднику отдела информационных технологий, телекоммуникации и связи.

3.4. Изложенные требования по оповещению администратора ИБ Общества об инцидентах ИБ должны включаться в должностной регламент сотрудников.

4. Реагирование на инциденты

4.1. После получения информации об инциденте ИБ администратор ИБ должен классифицировать инцидент по категории критичности. Для этого используются 4 категории классификации критичности инцидентов:

1 категория. Инцидент может привести к значительны негативным последствиям (ущербу) для информационных ресурсов (систем) или деловой репутации Общества и управляемых организаций.

2 категория. Инцидент может привести к негативным последствиям (ущербу) для информационных ресурсов (систем) или деловой репутации Общества и управляемых организаций.

3 категория. Инцидент может привести к незначительным негативным последствиям (ущербу) для информационных ресурсов.

4 категория. Инцидент не может привести к негативным последствиям (ущербу) для информационных ресурсов.

4.2. Для классификации инцидентов ИБ администратор ИБ может привлекать любых сотрудников Общества и управляемых организаций.

4.3. В зависимости от присвоенной категории критичности определяется приоритет и время реагирования по каждому типу инцидента ИБ. Сопоставление приоритетов и категорий инцидентов ИБ определяется по таблице:

приоритет	**категория критичности**	**время реагирования, часов, не более**
очень высокий	1	1
высокий	2	4
средний	3	8
низкий	4	48

4.4. В зависимости от приоритета инцидента ИБ, происходит выделение необходимых ресурсов для устранения (локализации) инцидента и его расследования.

4.5. В случае определения категории 1,2 администратор ИБ в обязательном порядке уведомляет отдел информационной безопасности Управления корпоративной защиты ООО «Газпром Межрегионгаз».

4.6. Для реагирования на инциденты ИБ категории 1,2,3 в Обществе оперативно должна быть создана специальная группа реагирования на инциденты ИБ (далее ГРИИБ), состоящая из следующих специалистов:

- Администратор ИБ;
- Администратор ИСПДн;
- пользователи профильного отдела Общества (по необходимости);
- в случае необходимости, для локализации инцидента ИБ приоритета «очень высокий», «высокий», администратор ИБ может привлекать в качестве экспертов специалистов отдела информационной безопасности Управления корпоративной защиты ООО «Газпром межрегионгаз».

4.7. ГРИИБ должны формироваться в зависимости от вида инцидента и необходимой степени участия каждой стороны.

4.8. Первостепенной задачей администратора ИБ (ГРИИБ) является сдерживание инцидента ИБ, то есть принятия всех необходимых мер для локализации инцидента ИБ и препятствующих его распространению.

4.9. В процессе реагирования на инцидент ИБ администратор ИБ (ГРИИБ) собирает всю относящуюся информацию для проведения расследования.

4.10. В процессе реагирования на инциденты ИБ сотрудники Общества и управляемых организаций обязаны неукоснительно следовать законодательству РФ и нормативных документов Общества.

5. Расследования инцидентов ИБ

5.1. Расследование инцидента ИБ включает проверку и сбор доказательств с серверов, сетевых устройств, ПК пользователей, а также традиционные мероприятия нетехнического характера, проводимые Администратором ИБ.

5.2. Целью расследования инцидента ИБ является раскрытие всех причинно-следственных связей и получение следующей информации:

- источники инцидента ИБ (нарушители);
- цели инцидента ИБ (информационные ресурсы, информация ограниченного доступа, персональные данные, репутация, др.);
- способы осуществления инцидента ИБ.

5.3. Сбор свидетельств инцидента ИБ представляет собой процедуру сбора фактов злонамеренных действий, направленных на реализацию угроз информационной безопасности. Причины, по которым необходим сбор свидетельств, рассматриваются как получение законных оснований для привлечения к ответственности лица или группы лиц за умышленное или непреднамеренное действие (бездействие) или попытку действия, направленную на реализацию угрозы ИБ в информационной системе Общества и управляемых организациях. Другая причина – формирование пакета для анализа уязвимости и совершенствования системы информационной безопасности Общества управляемых организациях.

5.4. Основной задачей по расследованию инцидентов ИБ ставится задача выявления (идентификации) нарушителя. В случае, если нарушителя не удается выявить в ходе анализа журналов систем, необходимо проводить мероприятия по сопоставлению фактов, уже проходивших инцидентов, для выявления нарушителя «по подчерку».

5.5. В ходе опроса или бесед с пользователями администратор ИБ должен уметь выявлять пользователей, не лояльно настроенных по отношению к выполняемой работе, средствам информатизации, руководству Общества. Такие пользователи потенциально могут выступать инициаторами реализации угроз безопасности.

5.6. При выявлении нарушителя по инцидентам ИБ категории 2,3 Администратор информационной безопасности в обязательном порядке предоставляет докладную записку заместителю генерального директора по корпоративной защите о назначении служебной проверки по фактам инцидента ИБ. При этом необходимо незамедлительно принять меры по отстранению

пользователя от работы на ПК, имеющего отношение к инциденту ИБ, для исключения дальнейшего развития инцидента и сохранения доказательной базы.

5.7. При выявлении нарушителя по инцидентам ИБ категории 1 заместитель генерального директора по корпоративной защите (председатель комиссии по защите информации) принимает решение о дальнейших действиях по отношению к нарушителю.

5.8. После выявления нарушителей по инцидентам категории 1,2,3 администратор ИБ (ГРИИБ) проводит ревизию ПК таких пользователей. В ходе проверки проводится анализ:

- записей в лог-журналах системы, ПО, указывающие на реализацию атаки (угрозы) или неизвестную ранее активность;
- историю интернет-обозревателей (включая файлы окружения, такие как cookies), сообщения электронной почты (включая прикрепленные файлы), в т.ч. удаленные;
- установленное или записанное ПО, не относящееся к основной деятельности работника Общества;
- наличие подозрительных файлов (включая графические или с незарегистрированными расширениями имен);
- проверка возможности у пользователя отключать средства защиты (антивирусная защита, средства НСД, очистка лог-журналов и т.д.);
- проверка возможности подключения пользователем неавторизованного носителя информации (в т.ч. соответствие предоставленных прав согласно заявке на доступ к ИР), осуществлять загрузку операционной системы с альтернативного носителя и т.д.;
- в определенных случаях, например, при явных признаках реализации угрозы данным пользователем, анализ может так же включать поиск удаленных файлов и областей, потерянных кластеров, свободного места, а также восстановление данных с обнаруженных в окружении носителей.

По результатам исследования необходимых узлов сети Администратором информационной безопасности (ГРИИБ) составляется акт и предоставляется на рассмотрение комиссии по защите информации. Акт также предоставляется в отдел экономической безопасности, в случае если назначена служебная проверка (расследование).

5.9. Администратор информационной безопасности (ГРИИБ) в обязательном порядке должен обеспечить хранение свидетельств расследования инцидента в любом виде (электронные журналы, снимки экрана, фотографии и т.д.) с соблюдением требований существующего законодательства. При этом необходимо учитывать, что:

– доказательства должны храниться в виде, пригодном для представления в судебные инстанции;
– время хранения устанавливается – не менее 2 лет.

5.10. После проведения расследования инцидента администратор ИБ проводит:

– переоценку угроз, повлекших возникновение инцидента ИБ;

- совместно с администраторами информационных ресурсов готовит перечень защитных мер для минимизации выявленных рисков, в случае повторения инцидента ИБ;
- актуализирует необходимые политики, включая настоящий документ.

6. Ответственность

Ответственность за осуществление контроля за соблюдением Порядка обнаружения и реагирования на инциденты информационной безопасности, за проведение мероприятий по исключению возникновения инцидентов ИБ, возлагается на Администратора ИБ.