УТВЕРЖДЕНО
приказом директора МУП «ОТС»
от 27 апреля 2018 г. № 244

ПОЛОЖЕНИЕ
по организации и проведению работ по защите персональных данных при их обработке в информационных системах персональных данных в МУП «ОТС»

1. Общие положении

1.1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПД), представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации и без использования таковых, в муниципальном унитарном предприятии «Оленегорские тепловые сети» муниципального образования город Оленегорск с подведомственной территорией Мурманской области (далее по тексту – МУП «ОТС»).

1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 года №152-ФЗ «О персональных данных», 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. Обработка персональных данных в МУП «ОТС» осуществляется на основе принципов, определённых ст. 5 Федерального закона от 27.07.2006 года №152-ФЗ «О персональных данных».

2. Порядок определения защищаемых информационных ресурсов

2.1. В соответствии с действующим законодательством РФ МУП «ОТС» является оператором персональных данных и обрабатывает информационные ресурсы, содержащие персональные данные, в пределах своих полномочий, установленных в соответствии с федеральным и областным законодательством, а также организационно-распорядительными документами МУП «ОТС» в целях обеспечения реализации прав субъектов персональных данных.

2.2. В соответствии с организационно-распорядительными документами в МУП «ОТС» определяется и утверждается содержание, состав и объём обрабатываемых персональных данных, закрепленный в Положении об обработке персональных данных в МУП «ОТС».

2.3. Настоящим Положением определяется и утверждается следующий перечень информационных систем персональных данных:

- «1С: Предприятие».

2.4. При проектирования вновь создаваемой или документировании ранее созданной (эксплуатируемой) информационной системы персональных данных определяются цели и содержание обработки персональных данных, определяемые действующим законодательством и утвержденные в Положении об обработке персональных данных в МУП «ОТС».

3. Основные условия проведения обработки персональных данных в информационных системах персональных данных

3.1. Работники МУП «ОТС», осуществляющие обработку персональных данных в информационных системах персональных данных, являются пользователями информационных систем персональных данных и обязаны принимать необходимые организационные и технические меры для их защиты.

3.2. Пользователи или иные лица, на законных основаниях получившие доступ к персональным данным, обязаны не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

3.3. Для планирования, разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных директором МУП «ОТС» назначается ответственное должностное лицо, а именно – инженер-программист МУП «ОТС».

3.4. В организации определяется перечень должностных лиц, допущенных к обработке персональных данных.

3.5. Должностными лицами МУП «ОТС», получающими доступ к персональным данным в информационных системах персональных данных, должна обеспечиваться конфиденциальность таких данных.

4. Обработка персональных данных в информационных системах персональных данных

4.1. Обработка персональных данных в информационных системах персональных данных осуществляется в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства Российской Федерации от 01.11.2012 № 1119, правовыми документами уполномоченных федеральных органов исполнительной власти.

4.2. Не допускается обработка персональных данных в информационных системах персональных данных при отсутствии:

- утвержденных организационно-распорядительных документов о порядке эксплуатации информационных систем персональных данных;
- сертифицированных средств защиты информации.

5. Порядок работы по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

5.1. Допуск работников МУП «ОТС» для работы на автоматизированных рабочих местах (далее – АРМ), предназначенных для обработки персональных данных, осуществляется в соответствии с Перечнем должностных лиц МУП «ОТС», допущенных к работе в информационных системах персональных данных, а именно:

- директор МУП «ОТС»;
- заместитель директора;
- заместитель директора по производству;
- заместитель директора по безопасности;
- главный инженер;
- главный бухгалтер;
- заместитель главного бухгалтера;
- бухгалтер;
- начальник финансово-экономического отдела;

- заместитель начальника финансово-экономического отдела;
- ведущий экономист;
- экономист;
- начальник юридического отдела;
- юрисконсульт;
- начальник производственно-технического отдела;
- кладовщик участка складского хозяйства;
- начальник отдела по энергонадзору;
- заместитель начальника по энергонадзору;
- начальник отдела по энергосбыту;
- инженер-энергетик;
- инженер по энергосбыту;
- начальник отдела кадров;
- специалист по кадрам;
- начальник контрактной службы;
- специалист по закупкам контрактной службы;
- инженер-программист;
- секретарь руководителя;
- кладовщик;
- руководители структурных подразделений (в отношении персональных данных работников, числящихся в соответствующих структурных подразделениях и в отношении персональных данных заявителей);
- специалисты подразделений МУП «ОТС» (в отношении персональных данных заявителей).

5.2. Работники МУП «ОТС» (далее – пользователи) имеют право в отведенное им рабочим распорядком или распоряжением директора МУП «ОТС», либо руководителем структурного подразделения время решать поставленные задачи в соответствии с полномочиями доступа к информационным ресурсам информационных систем персональных данных.

5.3. Доступ пользователям к ресурсам информационных систем персональных данных осуществляется на основании персональных паролей.

5.4. Пользователи, участвующие в автоматизированной обработке персональных данных и имеющие доступ к аппаратным средствам, программному обеспечению и данным информационных систем персональных данных, несут персональную ответственность за свои действия и обязаны:

- соблюдать установленные правила обеспечения безопасности информации при работе с программными средствами информационных систем персональных данных;
- знать и выполнять правила работы со средствами защиты информации, установленными на АРМ;
- обеспечивать конфиденциальность персональных паролей;
- выполнять требования по организации антивирусной защиты в полном объеме.

5.5. Пользователи обязаны извещать руководителя структурного подразделения МУП «ОТС» и инженера-программиста МУП «ОТС» в случае:

- при подозрении компрометации личных паролей;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств информационных систем персональных данных;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств;

- некорректного функционирования установленных на АРМ средств защиты информации;

- непредусмотренных конфигурацией АРМ отводов кабелей и подключенных устройств.

5.6. Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств информационных систем персональных данных или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

- осуществлять обработку персональных данных в присутствии посторонних лиц, не допущенных к защищаемой информации;

- записывать и хранить персональные данные и другую конфиденциальную информацию на неучтенных электронных носителях информации;

- оставлять АРМ без присмотра во включенном состоянии, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте персональный идентификатор, машинные носители и документы, содержащие защищаемую информацию;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению предпосылок или угроз утечки (неправомерной модификации) персональных данных;

- размещать средства отображения информации таким образом, чтобы создавалась возможность визуального считывания информации.

6. Порядок резервирования информации и восстановления работоспособности технических средств и программного обеспечения информационных систем персональных данных, а также средств защиты информации в информационных системах персональных данных

6.1. Для создания резервной копии конфиденциальной информации, обрабатываемой в информационных системах персональных данных, используются только учтённые (зарегистрированные) в установленном порядке носители информации.

6.2. Резервное копирование конфиденциальной информации обрабатываемой в информационных системах персональных данных, в том числе содержащей персональные данные производится автоматически под контролем инженера-программиста МУП «ОТС» ежедневно и (или) еженедельно.

6.3. Ответственность за проведение резервного копирования в информационных системах персональных данных в соответствии с требованиями настоящего Положения возлагается на инженера-программиста МУП «ОТС».

6.4. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения возлагается на инженера-программиста МУП «ОТС».

6.5. Ответственность за проведение мероприятий по восстановлению

работоспособности средств защиты информации возлагается на инженера-программиста МУП «ОТС».

7. Правила антивирусной защиты информационных систем персональных данных

7.1. Настоящий раздел определяет требования к организации защиты информационных ресурсов информационных систем персональных данных от разрушающего воздействия вредоносного программного обеспечения (компьютерных вирусов).

7.2. К использованию на АРМ информационных систем персональных данных допускаются только лицензионные антивирусные средства.

7.3. Установка и начальная настройка средств антивирусного контроля на АРМ информационных систем персональных данных осуществляется инженером-программистом МУП «ОТС».

7.4. Обновление антивирусных баз осуществляется автоматически с помощью антивирусного ПО.

7.5. Контроль работоспособности антивирусного ПО осуществляется инженером-программистом МУП «ОТС».

7.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

7.7. На АРМ запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации в информационных системах персональных данных.

7.8. При выявлении признаков наличия на АРМ вредоносных программ (нештатная работа программного обеспечения, появление графических и звуковых эффектов, искажений данных, немотивированная утрата массивов данных, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или с привлечением инженера-программиста МУП «ОТС») обязан провести внеочередную антивирусную обработку своего АРМ.

7.9. Ответственность за проведение мероприятий антивирусной защиты на АРМ информационных систем персональных данных возлагается на инженера-программиста МУП «ОТС».

8. Организация парольной защиты в информационных системах персональных данных

8.1. Настоящий раздел регламентирует организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных, а также контроль действий пользователей при работе с паролями.

8.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационных систем персональных данных возлагается на инженера-программиста МУП «ОТС».

8.3. Пользователь не имеет права сообщать личный пароль другим лицам.

8.4. Полная плановая смена паролей пользователей должна проводиться регулярно не реже одного раза в год.

8.5. В случае прекращения полномочий пользователя (увольнение, смена исполняемых функций внутри МУП «ОТС» и т.п.) удаление учетной записи пользователя

производится инженером-программистом МУП «ОТС».

9. Правила обновления общесистемного и прикладного программного обеспечения информационных систем персональных данных, а также технического обслуживания

9.1. Настоящий раздел регламентирует обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе информационных систем персональных данных.

9.2. Право внесения изменений в конфигурацию аппаратно-программных средств защищенных АРМ предоставляется инженеру-программисту МУП «ОТС».

9.3. Изменения в конфигурацию системных и прикладных программных средств, входящих в состав информационных систем персональных данных предусматривает:
установку (развертывание), обновление (замена), удаление на АРМе программных средств, необходимых для решения определенной задачи данной информационной системы персональных данных.

9.4. Обновления (модификация) и настройка программного обеспечения системы защиты информации в информационных системах персональных данных, внесение необходимых изменений в настройки средств защиты от несанкционированного доступа на АРМ, производится инженером-программистом МУП «ОТС». Работы производятся с ведома должностного лица, ответственного за эксплуатацию данной информационной системы персональных данных.

9.5. Установка и обновление программного обеспечения на АРМ производится только с оригинальных лицензионных дистрибутивных носителей, полученных установленным порядком, прикладного программного обеспечения - с эталонных копий программных средств.

9.6. При возникновении ситуаций, требующих передачи ПК для ремонта и обслуживания в специализированную сервисную организацию, носители информации, содержащие персональные данные, извлекаются и помещаются для хранения в специально отведённое для этих целей хранилище. Носители информации, извлечённые из системных блоков АРМов, и содержащие персональные данные выносу за пределы МУП «ОТС» не подлежат.

10. Осуществление контроля состояния защиты информации в информационных системах персональных данных

10.1. Контроль состояния защиты информации в информационных системах персональных данных – комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения техническими средствами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

10.2. Основными мероприятиям по контролю состояния защиты информации в информационных системах персональных данных являются:

- проверка соответствия условий эксплуатации информационных систем персональных данных требованиям нормативных правовых и организационно-распорядительных

документов по защите информации в информационных системах персональных данных;

- выявление возможных каналов утечки информации и внешних программно-технических воздействий на информацию, обрабатываемую в информационных системах персональных данных;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите информационных систем персональных данных от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите всех компонент информационных систем персональных данных;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в информационных системах персональных данных.

10.3. Контроль защиты информации осуществляется с учетом реальных условий эксплуатации информационных систем персональных данных как непосредственно на АРМах, в том числе с применением средств аудита обращений к информационной системе персональных данных, так и путём ознакомления с организационно-распорядительными документами на информационную систему персональных данных.

10.4. Основными видами технического контроля на объекте организации являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль эффективности защиты от несанкционированного доступа к информации и программно-технических воздействий на информацию.

10.5. Невыполнение предписанных мероприятий по защите персональных данных считается предпосылкой утечки (утраты) защищаемой информации.

10.6. В случае выявления в ходе контроля предпосылок утечки (утраты) защищаемой информации с целью установления обстоятельств их возникновения и причин невыполнения требований по указанию директора МУП «ОТС» может проводиться служебное расследование.

10.7. Контроль защиты информации осуществляется путем проведения как периодических плановых, так и внеплановых проверок объектов защиты. Периодические плановые проверки проводятся не реже одного раза в 3 года.

10.8. Обследование объектов информатизации проводится с целью определения соответствия объектов информатизации требованиям по защите информации, установленным «Аттестатом соответствия требованиям информационной безопасности». В ходе обследования объектов информатизации проверяется:

- соответствие класса информационной системы персональных данных условиям, сложившимся на момент проверки;
- выполнение требований предписаний на эксплуатацию технических средств и систем, организации электропитания и заземления;
- соответствие выполняемых в информационной системе персональных данных мероприятий по защите информации данным, изложенным в организационно-распорядительной документации;
- выполнение требований по защите автоматизированных систем от несанкционированного доступа;
- выполнение требований по антивирусной защите;
- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты;

10.9. Государственный контроль состояния защиты информации вправе осуществлять федеральные уполномоченные органы в соответствии с действующим законодательством Российской Федерации. В части обеспечения технической защиты информации (персональных данных) без применения криптографических средств государственный контроль осуществляет Федеральная служба технического и экспортного контроля Российской Федерации. В части защиты информации с применением криптографических средств государственный контроль осуществляет Федеральная служба безопасности Российской Федерации.

11. Ответственность должностных лиц

12.1. Работники МУП «ОТС», допущенные к обработке персональных данных в информационных системах персональных данных, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации и Мурманской области.