Приложение №1
к приказу ООО «Ферзь»
от «30» июля 2017 г. № 12

Положение
об обработке персональных данных в ООО «Ферзь»

I. Общие положения

1.1. Настоящее Положение об обработке персональных данных (далее - Положение) определяет порядок и условия обработки персональных данных в ООО «Ферзь» (далее по тексту - «Оператор»).

1.2. Целью настоящего Положения является обеспечение защиты прав граждан при обработке их персональных данных в сфере оказания услуг в сфере туризма, включая, но не ограничиваясь: по продвижению и реализации туристского продукта и\или отдельных туристских услуг.

1.3. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства РФ от 17.11.2007г. №781, Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства РФ от 15.09.2008г. №687, иными нормативно-правовыми актами.

1.4. Настоящее Положение вступает в силу с момента его утверждения Приказом директора предприятия и действует бессрочно, до замены его новым Положением. Все изменения в настоящее Положение вносятся Приказом директора предприятия.

1.5. В настоящем Положении используются следующие основные понятия:

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

К персональным данным могут относиться:

- сведения, содержащиеся в документе, удостоверяющем личность субъекта персональных данных (фамилия, имя, отчество, дата и место рождения, адрес регистрации, семейное положение и др.);

- информация, содержащаяся в трудовой книжке субъекта персональных данных;

- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;

- сведения, содержащиеся в документах воинского учета;

- сведения об образовании, квалификации или наличии специальных знаний или подготовки;

- информация медицинского характера, в случаях, предусмотренных законодательством;

- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;

- иная информация, относящаяся к прямо или косвенно определенному, или определяемому субъекту персональных данных;

- **информация –** сведения (сообщения, данные) независимо от формы их представления;

- **субъект персональных данных:**

- работник или иное физическое лицо, состоящее в договорных отношениях с Оператором;

- физическое лицо, обратившееся к Оператору с целью получения информации в сфере оказания услуг в сфере туризма;

- иное физическое лицо, в отношении которого Оператор обладает информацией, относящейся к персональным данным;

– **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;

- **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- **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;

- **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- **неавтоматизированная обработка персональных данных –** обработка персональных данных без использования средств автоматизации;

- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

- **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

II. Порядок и условия обработки персональных данных

2.1. Оператор осуществляет обработку персональных данных, исходя из следующих принципов:

- обработка персональных данных должна осуществляться на законной и справедливой основе;
- обработка персональных данных должна ограничиваться 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 должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных;
- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, либо договором, стороной которого является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Обработка персональных данных допускается в случаях, предусмотренных ФЗ «О персональных данных», в частности:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных

законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

4) обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных;

5) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

6) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц;

7) обработка персональных данных осуществляется в статистических целях, при условии обязательного обезличивания персональных данных;

8) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных).

2.3. Получение персональных данных осуществляется оператором лично у каждого субъекта персональных данных, либо у его представителя, имеющего соответствующие полномочия.

Персональные данные могут быть получены от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в подпунктах 2-8 пункта 2.2., подпунктах 1-7 пункта 2.7. настоящего Положения.

2.4. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных в письменной форме на основании заключаемого с этим лицом договора. В договоре с оператором должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных.

Лицо, осуществляющее обработку персональных данных по договору с оператором, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

2.5. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные

без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.6. Согласие на обработку персональных данных.

2.6.1. Субъект персональных данных дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

2.6.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в подпунктах 2-8 пункта 2.2, в пункте 2.7. настоящего Положения.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в подпунктах 2-8 пункта 2.2, в пункте 2.7. настоящего Положения, возлагается на оператора.

2.6.3. В случаях, предусмотренных ФЗ «О персональных данных», обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва;

9) подпись субъекта персональных данных.

2.6.4. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

2.6.5. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

2.7. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением следующих случаев:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные сделаны общедоступными субъектом персональных данных;

2.1.) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

3) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц;

6) обработка персональных данных осуществляется в соответствии с законодательством об исполнительном производстве Российской Федерации;

7) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

2.8. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность

(биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.

III. Способы обработки персональных данных

3.1. Оператор осуществляет неавтоматизированную и автоматизированную обработку персональных данных.

3.2. Неавтоматизированную и автоматизированную обработку персональных данных, включая доступ к соответствующим персональным данным, осуществляют работники оператора согласно перечню должностей, утвержденному Приказом директора предприятия.

3.3. Неавтоматизированная обработка персональных данных.

3.3.1. Обработка персональных данных, содержащихся в информационной системе либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

3.3.2. При неавтоматизированной обработке должны соблюдаться следующие требования:

1) Персональные данные при их обработке должны обособляться от иной информации, в частности путем фиксации на отдельных материальных носителях, в специальных разделах или на полях форм (бланков). Не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

2) Работники оператора должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, об особенностях и правилах такой обработки.

3) При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4) При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Вышеуказанные правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

5) Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

6) В отношении каждой категории персональных данных определяются места хранения персональных данных (материальных носителей), при этом хранение персональных данных, обработка которых осуществляется в различных целях, обеспечивается раздельно.

3.4. Автоматизированная обработка персональных данных.

3.4.1. При автоматизированной обработке должно быть обеспечено:

1) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

2) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

3) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

4) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5) постоянный контроль за обеспечением уровня защищенности персональных данных.

3.4.2. Перечень информационных систем, в которых оператор осуществляет обработку персональных данных, определен в Положении об обеспечении безопасности персональных данных при их обработке у Оператора.

3.4.3. Обеспечение безопасности персональных данных при их обработке в информационной системе осуществляется оператором в соответствии с Положением об обеспечении безопасности персональных данных при их обработке у Оператора.

IV. Права субъекта персональных данных

4.1. Субъект персональных данных вправе:

4.1.1. Получать информацию, касающуюся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ «О персональных данных»;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные ФЗ «О персональных данных» и другими федеральными законами.

Указанная информация должна быть представлена субъекту персональных данных оператором в доступной форме, и в ней не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за

исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Данная информация предоставляется субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью.

4.1.2. Обратиться повторно к оператору или направить ему повторный запрос в целях получения информации, указанной в подпункте 4.1.1. настоящего Положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если данная информация, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу.

4.1.3. Обратиться повторно к оператору или направить ему повторный запрос в целях получения вышеуказанной информации, а также в целях ознакомления с обрабатываемыми персональными данными до истечения тридцатидневного срока в случае, если такая информация и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

4.1.4. Требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

4.1.5. Обжаловать действия или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований ФЗ «О персональных данных» или иным образом нарушает его права и свободы.

4.1.6. Защищать свои права и законные интересы, в том числе на возмещение убытков и (или) компенсацию морального вреда, в судебном порядке.

V. Права и обязанности оператора

5.1. Оператор вправе:

5.1.1. Отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным подпунктами 4.1.2, 4.1.3. настоящего Положения. Такой отказ должен быть мотивированным.

5.2. Оператор обязан:

5.2.1. При сборе персональных данных предоставить субъекту персональных данных по его просьбе информацию, предусмотренную подпунктом 4.1.1. настоящего Положения.

5.2.2. Разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с ФЗ «О персональных данных».

5.2.3. Если персональные данные получены не от субъекта персональных данных, до начала обработки таких персональных данных предоставить субъекту персональных данных следующую информацию:

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные настоящим Положением права субъекта персональных данных;
- источник получения персональных данных.

Оператор освобождается от обязанности предоставить субъекту персональных данных указанную информацию в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- предоставление субъекту персональных данных указанной информации нарушает права и законные интересы третьих лиц.

5.2.4. Сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

5.2.5. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя, дать в письменной форме мотивированный ответ в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя, либо с даты получения запроса субъекта персональных данных или его представителя.

5.2.6. Предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

5.2.7. Сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

5.2.8. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по договору с оператором) с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по договору с оператором) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

5.2.9. В случае подтверждения факта неточности персональных данных, на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по договору с оператором) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

5.2.10. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по договору с оператором, в срок, не превышающий трех рабочих дней с даты этого выявления, прекратить

неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по договору с оператором.

5.2.11. В случае, если обеспечить правомерность обработки персональных данных невозможно, в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожить такие персональные данные или обеспечить их уничтожение.

5.2.12. Уведомить субъекта персональных данных или его представителя об устранении допущенных нарушений или об уничтожении персональных данных, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также уведомить указанный орган.

5.2.13. В случае достижения цели обработки персональных данных прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по договору с оператором) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по договору с оператором) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных.

5.2.14. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по договору с оператором) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по договору с оператором) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных.

5.2.15. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в подпунктах 5.2.11, 5.2.13, 5.2.14. настоящего Положения, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по договору с оператором) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.2.16. Назначить лицо, ответственное за организацию обработки персональных данных, которое обязано:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Указанное лицо непосредственно получает указания от директора предприятия и подотчетно ему.

5.2.17. Принимать необходимые правовые, организационные и технические меры по обеспечению безопасности персональных данных.

5.2.18. Осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных ФЗ «О персональных данных» и принятым в соответствии с ним локальным нормативным актам: настоящему Положению, Положению об обеспечении безопасности персональных данных при их обработке у Оператора.

5.2.19. Обеспечить неограниченный доступ к настоящему Положению, к сведениям о реализуемых требованиях к защите персональных данных на предприятии путем опубликования указанных документов в сети Интернет на официальном сайте Оператора, а также путем предоставления данных документов на основании письменных запросов заинтересованных лиц.

5.2.20. Производить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным законом.

5.2.21. Уведомить уполномоченный орган по защите прав субъектов персональных данных до начала обработки персональных данных о своем намерении осуществлять обработку персональных данных, в порядке, предусмотренном ФЗ «О персональных данных», за исключением следующих случаев:

1) персональные данные обрабатываются в соответствии с трудовым законодательством;

2) персональные данные получены оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) сделанных субъектом персональных данных общедоступными;

4) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

5) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях.

VI. Особенности обработки персональных данных работников Предприятия

6.1. При обработке персональных данных работников Предприятия оператор обязан:

1) осуществлять обработку персональных данных работника исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) при определении объема и содержания обрабатываемых персональных данных работника руководствоваться Конституцией Российской Федерации, трудовым и иным законодательством;

3) получать все персональные данные работника у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) не получать и не обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, за исключением когда от работника получено письменное согласие;

5) не получать и не обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством;

6) при принятии решений, затрагивающих интересы работника, не основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) ознакомить работников Предприятия с документами, устанавливающими порядок обработки персональных данных, их правами и обязанностями в области защиты персональных данных, под роспись.

6.2. При передаче персональных данных работника оператор должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получивших персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности);

- осуществлять передачу персональных данных работников в пределах Предприятия в соответствии с настоящим Положением;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функции.

VII. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

7.1. Лица, виновные в нарушении требований ФЗ «О персональных данных», несут дисциплинарную и материальную, гражданско-правовую, административную, уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

7.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных ФЗ «О персональных данных» и настоящим Положением, а также требований к защите персональных данных, установленных в соответствии с ФЗ «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации.

Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Приложения к настоящему Положению:

1. Приложение №1 «Согласие на обработку персональных данных»;
2. Приложение №2 «Согласие на передачу персональных данных третьему лицу»;
3. Приложение №3 «Отзыв согласия на обработку персональных данных»;
4. Приложение №4 «Отзыв согласия на передачу персональных данных третьему лицу»;
5. Приложение №5 «Запрос»;
6. Приложение №6 «Положение об обеспечении безопасности персональных данных при их обработке у Оператора».

Приложение №1

Кому: _____

от _____,
(Ф.И.О. субъекта персональных данных, адрес, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе)

_____,
(Ф.И.О. представителя субъекта персональных данных, адрес, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего его полномочия)

СОГЛАСИЕ
на обработку персональных данных

В соответствии со ст. ФЗ "О персональных данных" я, _____,
(Ф.И.О. субъекта персональных данных/его представителя)
даю согласие_____
(наименование оператора)

на _____ обработку:
(способ обработки: автоматизированный/неавтоматизированный)
_____
(перечень действий по обработке персональных данных)
персональных данных
_____
(перечень персональных данных субъекта персональных данных)
в целях_____.

Срок действия согласия_____.

Настоящее согласие может быть отозвано мной в письменной форме.

_____ _____
(подпись) (фамилия, инициалы)

«___» _____ 20__ г.
(дата)

Приложение №2

Кому: _____

от _____,
(Ф.И.О. субъекта персональных данных, адрес, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе)

_____,
(Ф.И.О. представителя субъекта персональных данных, адрес, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего его полномочия)

СОГЛАСИЕ
на передачу персональных данных третьему лицу

В соответствии со ст. ФЗ "О персональных данных" я, _____,
(Ф.И.О. субъекта персональных данных/его представителя)
даю согласие_____
(наименование оператора)
на передачу_____
(наименование третьего лица)
персональных данных_____
(перечень персональных данных субъекта персональных данных)
для _____ обработки:
(способ обработки: автоматизированный/неавтоматизированный)
_____
(указать перечень действий по обработке персональных данных)

в целях_____.

Срок действия согласия_____.

Настоящее согласие может быть отозвано мной в письменной форме.

_____ _____
(подпись) (фамилия, инициалы)
«___» _____ 20__ г.
(дата)

Приложение №3

Кому: _____

от _____,
(Ф.И.О. субъекта персональных данных, адрес, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе)

_____,
(Ф.И.О. представителя субъекта персональных данных, адрес, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего его полномочия)

Отзыв
согласия на обработку персональных данных

Я, _____,
(Ф.И.О. субъекта персональных данных/его представителя)
отзываю данное мной согласие на обработку персональных данных.

_____ _____
(подпись) (фамилия, инициалы)

«___» _____ 20__ г.
(дата)

Приложение №4

Кому: _____

от _____,
(Ф.И.О. субъекта персональных данных, адрес, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе)

_____,
(Ф.И.О. представителя субъекта персональных данных, адрес, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего его полномочия)

Отзыв
согласия на передачу персональных данных третьему лицу

Я, _____,
(Ф.И.О. субъекта персональных данных/его представителя)
отзываю данное мной согласие на передачу персональных данных _____.
(указать наименование третьего лица)

_____ _____
(подпись) (фамилия, инициалы)

«___» _____ 20__ г.
(дата)

Приложение №5

Кому: _____

от _____,
(Ф.И.О. субъекта персональных данных/его представителя, адрес, номер основного документа, удостоверяющего личность субъекта персональных данных/его представителя, сведения о дате выдачи указанного документа и выдавшем его органе; для представителя – реквизиты доверенности или иного документа, подтверждающего его полномочия)

Запрос

В соответствии со ст. 14 ФЗ «О персональных данных» прошу предоставить следующую информацию, касающуюся обработки персональных данных _____:
(Ф.И.О. субъекта персональных данных)

_____
(указать конкретную информацию, касающуюся обработки персональных данных)
_____

_____.

Сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором: _____

_____ _____
(подпись) (фамилия, инициалы)

«___» _____ 20__ г.
(дата)

Приложение № 6

Положение об обеспечении безопасности персональных данных при их обработке у Оператора

1. Общие положения

1.1. Настоящее Положение об обеспечении безопасности персональных данных при их обработке у Оператора (далее – Положение) определяет меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Целью настоящего Положения является обеспечение защиты прав граждан при обработке их персональных данных в информационных системах персональных данных в сфере оказания услуг в сфере туризма, включая, но не ограничиваясь: по продвижению и реализации туристского продукта и\или отдельных туристских услуг.

1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 17.11.2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и иными нормативно-правовыми актами.

1.3. Настоящее Положение вступает в силу с момента его утверждения приказом Оператора и действует бессрочно до замены его новым Положением. Все изменения в настоящее Положение вносятся приказом Оператора.

2. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.

2.1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры и обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2.2. Обеспечение безопасности персональных данных достигается, в частности:

2.2.1. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2.2.2 Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к

защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных.

2.2.3. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.2.4. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

2.2.5. Учетом машинных носителей персональных данных.

2.2.6. Обнаружение фактов несанкционировнного доступа к персональным данным и принятием мер.

2.2.7. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.2.8. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

2.2.9. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3.1. Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

3.2. Определение угроз безопасности персональных данных осуществляется в модели угроз безопасности персональных данных соответствии с Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России от 15.02.2008 г.

4. Информационные системы персональных данных.

4.1. На предприятии используются следующие информационные системы персональных данных:

Наименование системы	Подразделение предприятия	Тип базы данных	Доступ в интернет	Объем данных	Класс системы
1С «Бухгалтерия»	Бухгалтерия	Многопользовательская, SQL-сервер	Да, используется Крипто Про	1000 – 100000	Класс К3
1С «Зарплата и кадры»	Отдел кадров, расчетный отдел	Многопользовательская, SQL-сервер	Да, используется Крипто Про	< 1000	Класс К3
Файлы Microsoft Word, Microsoft Excel	Секретариат, производственно-технический отдел, договорной отдел	Разрозненные файлы	Нет	1000 – 100000	Класс К3

4.2. Используемые информационные системы персональных данных классифицированы по классу К3 в соответствии с Приказом ФСТЭК, ФСБ, Мининформсвязи России от 13.02.08 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

4.3. Классификация информационных систем персональных данных проведена по результатам анализа следующих исходных данных:

1) Категория обрабатываемых в информационной системе персональных данных: 2 (в информационной системе 1С «Зарплата и кадры») - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни; 3 (в прочих информационных системах предприятия) – персональные данные, позволяющие идентифицировать субъекта персональных данных.
2) Объем персональных данных, обрабатываемых в системе: 3 – менее 1000 субъектов персональных данных в информационной системе 1С «Зарплата и кадры»; 2 - от 1000 до 100000 субъектов персональных данных в прочих информационных системах предприятия.
3) По заданным оператором характеристикам безопасности персональных данных информационные системы персональных данных предприятия являются типовыми информационными системами, требующими обеспечения конфиденциальности персональных данных.
4) По структуре информационные системы персональных данных являются комплексами автоматизированных рабочих мест, объединенными в единую информационную систему средствами связи без использования технологии удаленного доступа, т.е. являются локальными.

5) По наличию подключения к сетям общего пользования информационные системы персональных данных предприятия относятся к системам, имеющим подключения.
6) По режиму обработки персональных данных информационные системы персональных данных предприятия относятся к многопользовательским системам.
7) По разграничению прав доступа пользователей информационные системы персональных данных предприятия относится к системам с разграничением прав доступа.
8) Информационные системы персональных данных предприятия являются системами, все технические средства которых находятся в пределах Российской Федерации.

4.4. Результаты классификации информационных систем персональных данных предприятия оформлены Актом о присвоении класса информационным системам персональных данных Оператора.

4.5. Класс информационной системы может быть пересмотрен: по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы; по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

5. Перечень автоматизированных рабочих мест, используемых для обработки персональных данных, и работников, ответственных за их безопасность при обработке на автоматизированных рабочих местах.

5.1. Перечень автоматизированных рабочих мест (далее – АРМ), на которых осуществляется обработка персональных данных в составе информационных систем персональных данных, утверждается приказом Оператора.

5.2. Перечень АРМ, на которых осуществляется обработка персональных данных, своевременно корректируется и дополняется программистами предприятия, ответственными за безопасность персональных данных при их автоматизированной обработке.

5.3. Ответственным за безопасность персональных данных при обработке их на каждом отдельном АРМ является работник, осуществляющий обработку персональных данных с использованием этого АРМ. Данный работник указывается в перечне АРМ, используемых для обработки персональных данных, в графе «Ответственный работник». В тех случаях, когда одно АРМ используют несколько работников, все они перечисляются в числе ответственных за безопасность персональных данных при работе на этом АРМ.

6. Перечень персональных данных, обрабатываемых в информационных системах персональных данных

6.1. В информационных системах персональных данных предприятия обрабатываются следующие персональные данные субъектов, не являющихся работниками предприятия, позволяющие идентифицировать данного субъекта персональных данных:

- Фамилия, имя отчество;
- Дата рождения;
- Контактный телефон;
- Адрес регистрации или фактического проживания;
- Паспортные данные.

6.2. В информационной системе персональных данных 1С «Зарплата и кадры» помимо персональных данных, позволяющих идентифицировать работника предприятия, могут обрабатываться прочие персональные данные работников предприятия:

- Информация об образовании;
- Информация о трудовой деятельности;
- Информация о трудовом стаже;
- Семейное положение и состав семьи;
- Информация о знании иностранных языков;
- Информация о заработной плате;
- Данные о трудовом договоре;
- Сведения о воинском учете;
- ИНН;
- Данные о повышении квалификации и аттестации, о наградах, медалях и поощрениях;
- Информация о приеме на работу, перемещении по должности, увольнениях, выходах в отпуск;
- Информация о пенсионном обеспечении

и прочие персональные данные, за исключением персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

7. Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

7.1. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает

нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

7.2. Уровень требований, предъявляемых по обеспечению безопасности персональных данных, обрабатываемых в информационных системах предприятия, зависит от состава актуальных угроз и класса информационной системы персональных данных. Для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных класса 3 система защиты персональных данных должна включать:

- управление доступом;
- регистрацию и учет;
- обеспечение целостности персональных данных;
- криптографическую защиту;
- антивирусную защиту;
- предотвращение и обнаружение вторжений.

7.3. Система управления доступом реализована в информационных системах персональных данных предприятия и позволяет разграничивать доступ пользователей к отдельным объектам системы и отдельным группам персональных данных.

7.3.1. Пользователи информационных систем персональных данных объединены в группы, обладающие определенными ролями в процессе обработки данных. Роли определяют, какими правами доступа обладают пользователи информационных систем персональных данных.

7.3.2. Аутентификация пользователя при доступе к информационным системам персональных данных осуществляется с помощью уникального идентификатора пользователя (логина) и пароля. Пароль должен иметь цифробуквенную структуру, т.е. состоять одновременно из цифр и букв в русской или латинской раскладке клавиатуры. Пароль не может быть короче 6 символов. Пароли меняются регулярно 1 раз в квартал у всех пользователей информационных систем персональных данных.

7.3.2.1. Ответственным за неразглашение пароля назначается пользователь информационной системы персональных данных.

7.3.2.2. Смену пароля пользователя информационной системы персональных данных осуществляют программисты предприятия, ответственные за безопасность персональных данных при их автоматизированной обработке. Смена пароля протоколируется в «Журнале изменений паролей пользователей информационных систем персональных данных» под роспись пользователя.

7.3.2.3. В случае, если создалась угроза компрометации пароля пользователя информационных систем персональных данных, пользователь обязан

незамедлительно обратиться к программистам предприятия, ответственным за безопасность персональных данных при их автоматизированной обработке, для внеплановой смены пароля.

7.3.3. Физический доступ посторонних лиц к рабочим местам пользователей информационных систем персональных данных запрещен. Персональные данные обрабатываются в отдельных помещениях, а пользовательские терминалы имеют функцию автоблокировки по истечению заданного времени бездействия.

7.3.4. Хранение централизованных баз данных информационных систем персональных данных осуществляется на основных серверах предприятия, расположенных в специально выделенном, закрытом помещении (серверной) со строго ограниченным доступом. Доступ в серверную имеют только программисты предприятия, ответственные за безопасность персональных данных при их автоматизированной обработке. Сетевой доступ к базам данных информационных систем персональных данных разграничен по правам доступа ролей пользователей, ведущих обработку персональных данных.

7.3.5. Доступ в глобальную сеть Интернет на рабочих местах пользователей информационных систем персональных данных запрещен на уровне настроек автоматизированного рабочего места, а также на уровне прокси-сервера предприятия, осуществляющего централизованный доступ в Интернет. Использование GSM-модемов на рабочих местах пользователей информационных систем персональных данных запрещено.

7.4. Система регистрации и учета реализована в информационных системах персональных данных предприятия в виде электронных журналов учета действий пользователя, в которых регистрируются подлежащие учету действия пользователя: дата и время доступа пользователя к информационной системе персональных данных, тип объекта информационной системы, к которому был осуществлен доступ, вид действия, которое было произведено с объектом информационной системы.

7.5. Обеспечение целостности персональных данных при обработке в информационных системах персональных данных достигается применением процедуры автоматического многократно дублированного резервного копирования персональных данных с возможностью их быстрого восстановления в случае их изменения, повреждения, блокирования или уничтожения в следствие технологической аварии или несанкционированного доступа.

7.5.1. Резервное копирование персональных данных осуществляется автоматически в конце каждого рабочего дня.

7.5.2. Резервные копии персональных данных дублируются на основных серверах предприятия, а также на компьютере программиста предприятия, ответственного за резервное копирование персональных данных. Резервные копии персональных

данных хранятся в виде электронных архивов в течение длительного времени, что позволяет в случае необходимости восстановить их с разной степенью актуальности. Файловый и сетевой доступ к резервным копиям персональных данных ограничен программистами предприятия, ответственными за резервное копирование и безопасность персональных данных при их автоматизированной обработке.

7.5.3. Программист предприятия, ответственный за резервное копирование персональных данных, может в течение рабочего дня создавать резервные копии персональных данных по своему усмотрению в целях предотвращения их изменения, повреждения или уничтожения.

7.5.4. Резервные копии персональных данных могут быть записаны на твердотельные диски (DVD-ROM) для долговременного хранения. Запись резервной копии персональных данных на твердотельный диск осуществляется программистом предприятия, ответственным за резервное копирование персональных данных. Факт записи фиксируется в «Журнале учета записей резервных копий персональных данных для долговременного хранения». Резервные копии персональных данных на твердотельных дисках хранятся в специально оборудованном, закрытом помещении с ограниченным доступом.

7.6. Криптографическая защита персональных данных в информационных системах персональных данных предприятия применяется в случае передачи персональных данных по сетям общего пользования для обработки в сторонние организации, с которыми заключены соответствующие договоры. Криптографическая защита персональных данных основана на применении электронно-цифровой подписи и сертифицированного криптографического комплекса Крипто Про.

7.7. Антивирусная защита персональных данных обеспечена применением антивирусного программного комплекса на всех компьютерах предприятия. Обновление антивирусных баз осуществляется ежедневно автоматически под контролем программиста предприятия, ответственного за антивирусную защиту.

7.8. Предотвращение вторжений в электронно-вычислительную сеть предприятия и информационные системы персональных данных обеспечено следующими мерами:

- разграничение доступа пользователей к компьютерам с использованием логина и пароля;
- разграничение доступа пользователей к объектам информационных систем согласно ролям пользователей;
- автоматическая блокировка неиспользуемых длительное время терминалов;
- использование специально оборудованного, закрытого помещения с ограниченным доступом для содержания центральных серверов предприятия и хранения резервных копий персональных и технологических данных;

- использование брандмауэров на персональных компьютерах пользователей и серверах предприятия;
- исключение непосредственного доступа в глобальную сеть Интернет рабочих мест, на которых ведется обработка персональных данных, и серверов предприятия;
- применение криптографической защиты в сеансе обмена данными через глобальную сеть Интернет в тех случаях, когда это необходимо для передачи персональных данных;
- использование централизованного прокси-сервера, брандмауэра и технологии трансляции сетевых адресов (NAT) для разграничения и контроля доступа пользователей в Интернет, не ведущих непосредственную обработку персональных данных, а также предотвращения непосредственного доступа из сети Интернет в локально-вычислительную сеть предприятия;
- использование брандмауэра и технологии трансляции сетевых адресов (NAT) для организации доступа пользователей глобальной сети Интернет к веб-серверу предприятия (сервер скрыт внутри сети от несанкционированного доступа);
- регулярный мониторинг уязвимостей используемого программного обеспечения программистами предприятия, ответственными за безопасность персональных данных при их автоматизированной обработке, и обновление его в случае обнаружения критических уязвимостей;
- регулярное резервное копирование системной технологической информации: файлов конфигурации, журналов регистрации, базы данных контроллеров домена, веб-сервера предприятия и прочей технологической информации.

Для обнаружения вторжений программистами предприятия, ответственными за безопасность персональных данных при их автоматизированной обработке, проводится регулярный анализ файлов регистрации прокси-сервера, веб-сервера и основных серверов предприятия.

8. Осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных

8.1. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных при обработке их в информационных системах персональных данных предприятия осуществляют программисты предприятия, ответственные за безопасность персональных данных при их автоматизированной обработке.

8.2. Программисты предприятия, ответственные за безопасность персональных данных при их автоматизированной обработке, обеспечивают:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным;

- своевременное обнаружение фактов несанкционированного доступа к персональным данным или же их изменения, повреждения, блокировки или уничтожения;
- осуществление режима разграничения доступа пользователей к информационным системам персональных данных;
- осуществление контроля за плановой сменой паролей пользователей, осуществляющих обработку персональных данных;
- недопущение воздействий на технические средства автоматизированной обработки персональных данных, в результате которых может быть нарушено их функционирование;
- поддержание в работоспособном состоянии и своевременное обновление технических и программных средств автоматизированной обработки персональных данных;
- возможность незамедлительного восстановления персональных данных из резервных копий в случаях их изменения, повреждения, блокировки или уничтожения вследствие технологических неисправностей или несанкционированного доступа;
- контроль за осуществлением регулярного резервного копирования персональных данных;
- формирование и поддержание в актуальном состоянии перечней информационных систем персональных данных и автоматизированных рабочих мест, используемых для обработки персональных данных, а также списков работников, ответственных за безопасность персональных данных при их обработке на конкретном автоматизированном рабочем месте;
- проведение инструктажа работников по безопасности персональных данных при обработке их на автоматизированных рабочих местах;
- прочий контроль за соблюдением мер, направленных на обеспечение защиты персональных данных при их обработке в информационных системах персональных данных.

9. Права и обязанности работников, осуществляющих обработку персональных данных на автоматизированных рабочих местах.

9.1. Работник, осуществляющий обработку персональных данных на автоматизированном рабочем месте, обязан:

- знать и выполнять требования действующих нормативных актов предприятия в сфере обработки персональных данных;
- знать и соблюдать установленные требования по условиям и порядку обработки персональных данных, учету, обеспечению безопасности персональных данных;
- соблюдать требования правил создания и использования паролей доступа к информационным системам персональных данных, в частности, обеспечивать: неразглашение своего индивидуального логина и пароля, в том числе в письменном виде в качестве записок-напоминаний, пометок и т.п., своевременную плановую смену пароля или внеплановую в случае угрозы его разглашения;

- обеспечивать недопущение за свое рабочее место посторонних лиц, а также работников, не имеющих доступ к обработке персональных данных на его рабочем месте;
- экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами, жалюзи на оконных проемах должны быть закрыты;
- блокировать терминал своего рабочего места при его покидании путем нажатия комбинации Win+L на клавиатуре либо комбинации Ctrl+Alt+Del и выбора опции «Блокировать компьютер»;
- незамедлительно извещать программистов предприятия, ответственных за безопасность персональных данных при их автоматизированной обработке, в случае выявленных фактов изменения, повреждения, блокирования или уничтожения персональных данных.

9.2. Работнику, осуществляющему обработку персональных данных на автоматизированном рабочем месте, запрещается:

- разглашать персональные данные третьим лицам;
- копировать персональные данные на внешние носители либо общедоступные сетевые ресурсы без разрешения своего непосредственного руководителя;
- самостоятельно вмешиваться в функционирование аппаратных и программных составляющих своего автоматизированного рабочего места, устанавливать программы, драйверы, GSM-модемы, подключать мобильные устройства и тому подобное оборудование;
- несанкционированно, без разрешения своего непосредственного руководителя и консультации с программистами предприятия, ответственными за безопасность персональных данных при их автоматизированной обработке, открывать общий доступ к папкам на своем автоматизированном рабочем месте;
- отключать или блокировать средства защиты информации такие, как антивирусная система и сетевой брандмауэр;
- хранить и обрабатывать на своем автоматизированном рабочем месте информацию личного характера и прочую информацию, не имеющую непосредственного отношения к должностным обязанностям работника;
- привлекать посторонних лиц для производства ремонта или настройки своего автоматизированного рабочего места.

9.3. Работник, осуществляющий обработку персональных данных на автоматизированном рабочем месте, имеет право получать инструктаж по безопасности персональных данных у программистов предприятия, ответственных за безопасность персональных данных при их автоматизированной обработке, а также обращаться к ним по иным вопросам в целях обеспечения безопасности персональных данных.