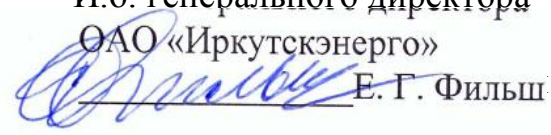
СТП 011.563.008-2011

Стандарт предприятия

О защите персональных данных

Взамен СТП 001.089.008-2005

УТВЕРЖДАЮ
И.о. генерального директора
ОАО «Иркутскэнерго»

_____ Е. Г. Фильш
_____
(дата)

Наименование подразделения-разработчика: Менеджер системы информационной безопасности

Введен в действие приказом «Иркутскэнерго»
от 30.12.2011 № 586

ОАО «Иркутскэнерго»

Содержание

Введение

Настоящий стандарт предприятия (СТП) разработан на основании плана стандартизации ОАО «Иркутскэнерго».

1. Область применения

1.1. Настоящий стандарт устанавливает в ОАО «Иркутскэнерго» общие требования к обеспечению безопасности персональных данных обрабатываемых в ОАО «Иркутскэнерго» с использованием средств автоматизации или без использования таких средств, основные задачи, функции и права подразделений, в обязанности которых входит проведение работ по организации защиты персональных данных.

1.2. Настоящий стандарт предприятия распространяется на все подразделения ОАО «Иркутскэнерго». Работники ОАО «Иркутскэнерго», осуществляющие обработку персональных данных, должны быть ознакомлены с настоящим стандартом.

1.3. Настоящий стандарт предприятия входит в состав нормативных документов системы управления ОАО «Иркутскэнерго».

2. Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие документы:

- Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных».
- Трудовой кодекс РФ.
- Указ Президента Российской Федерации от 06.03.1997 г. №188 «Об утверждении перечня сведений конфиденциального характера».
- СТП 011.473.128-2010 Политика в области информационной безопасности.
- СТП 001.039.103-2008 Термины и определения в области информационных технологий и информационной безопасности.
- СТП 011.473.140-2011 Система управления информационной безопасностью.
- СТП 011.473.152-2011 Аудит информационной безопасности.
- СТП 011.105.128-2010 Политика информационной безопасности.
- СТП 001.042.100-2007 Политика в области управления персоналом.
- СТП 00.04.01.089.0001-2003 Регламент отбора и найма персонала.
- СТП 001.089.036-2006 Регламент проведения оценки по технологии АЦ.
- СТП 011.534.043-2012 О пропускном и внутриобъектовом режиме.
- СТП 011.473.134-2010 Управление доступом к информационным ресурсам информационных систем.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн, утвержденная ФСТЭК России 14 февраля 2008 г.
- Постановление Правительства Российский Федерации от 17.11.2007 г. №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
- Постановление Правительства Российский Федерации от 15.09.2008 г. №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 г. 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».
- Положение «О методах и способах защиты информации в информационных системах персональных данных», утвержденное Приказом Федеральной службы по техническому и экспортному контролю 05.02.2010 г. №58.

3. Сокращения и определения

В настоящем стандарте используются сокращения и определения из СТП 001.039.103-2008 «Термины и определения в области информационных технологий и информационной безопасности» и Федерального закона от 27.07.2006 года №152-ФЗ «О персональных данных».

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

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

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

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

Классификация информационных систем персональных данных - это присвоение класса системам с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их раскрытия и распространения без согласия субъекта персональных данных или наличия иного законного основания;

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.

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

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

Специальные категории персональных данных - сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

Биометрические персональные данные - сведения, которые характеризуют физиологически и биологические особенности человека, на основании которых можно установить его личность;

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

Нештатная ситуация - ситуация, при которой процесс обработки персональных

данных или состояние информационной системы выходит за рамки нормального функционирования и может привести к нарушению конфиденциальности (целостности, доступности) указанных данных;

Третье лицо - лицо, которому поручена обработка персональных данных на основании заключаемого с ним договора либо лицо, которое запрашивает персональные данные не относящиеся к нему;

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

ПДн - персональные данные;
ИСПДн - информационная система персональных данных;
ИБ - информационная безопасность.

4. Основные положения

4.1. Принципы обработки персональных данных

Обработка персональных данных осуществляется на основе принципов:

4.1.1 законности целей и способов обработки персональных данных;

4.1.2 соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;

4.1.3 соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4.1.4 достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

4.1.5 недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

4.2. Способы обработки и перечень действий с персональными данными

4.2.1 ОАО «Иркутскэнерго» может осуществлять обработку персональных данных с использованием средств автоматизации, а также без использования таких средств.

4.2.2 Перечень действий с персональными данными, которые могут осуществляться ОАО «Иркутскэнерго» при обработке персональных данных субъектов: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение.

4.2.3 При необходимости ОАО «Иркутскэнерго» производит уведомление уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных, согласно статье 22 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных».

5. Субъекты и категории персональных данных, цели обработки

5.1. Категории субъектов персональных данных

5.1.1 ОАО «Иркутскэнерго» может осуществляться обработка персональных данных следующих категорий субъектов персональных данных:

– физические лица, состоящие или состоявшие в договорных и иных отношениях с ОАО «Иркутскэнерго»;

– работники, состоящие или состоявшие в трудовых отношениях с ОАО «Иркутскэнерго».

5.2. Категории персональных данных субъектов персональных данных

5.2.1 В ОАО «Иркутскэнерго» проводится классификация персональных данных в соответствии со степенью тяжести последствий потери свойств безопасности персональных данных для субъектов персональных данных. Выделяются следующие категории персональных данных:

– персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к специальным категориям персональных данных;

– персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к биометрическим персональным данным;

– персональные данные, которые не могут быть отнесены к категориям персональных данных перечисленных в п.5.4.1 настоящего СТП, а так же к персональным данным в общедоступных источниках или обезличенным персональным данным;

– персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к обезличенным персональным данным или расположенные в общедоступных источниках.

5.2.2 В информационных системах ОАО «Иркутскэнерго» не должна осуществляться обработка персональных данных относящихся к: специальным категориям персональных данных, касающимся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны в ОАО «Иркутскэнерго» только с его письменного согласия.

5.2.3 Обработка всех категорий персональных данных может осуществляться только в установленных законодательством случаях. Начало обработки, а также процедуры сбора, передачи, обезличивания, блокирования, удаления, уничтожения персональных данных выполняются по служебной записке руководителя структурного подразделения, согласованной с Дирекцией по защите активов.

5.3. Цели обработки персональных данных

5.3.1 В ОАО «Иркутскэнерго» определены следующие цели обработки персональных данных:

– обработка персональных данных работников ОАО «Иркутскэнерго» может осуществляться с целью организации учета работников ОАО «Иркутскэнерго», содействия работникам в трудоустройстве, обучения, страхования, продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества: пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, иными федеральными законами, а также локальными актами ОАО «Иркутскэнерго».

– обработка персональных данных физических лиц, состоявших или состоящих в договорных и иных отношениях с ОАО «Иркутскэнерго», осуществляется с целью

осуществления уставных видов деятельности.

5.4. Объем и содержание персональных данных

5.4.1 Для целей обработки персональных данных определены следующие объем и содержание персональных данных:

– объем и содержание персональных данных работников ОАО «Иркутскэнерго»: фамилия, имя, отчество, дата и место рождения, пол, гражданство, паспортные данные или данные иного документа удостоверяющего личность (серия, номер, когда и кем выдан), сведения, характеризующие физиологические особенности (изображение лица), адрес места жительства, контактная информация, сведения об образовании, специальности, квалификации и о наличии специальных знаний и специальной подготовки, сведения о трудовой деятельности, сведения о трудовом и общем стаже, заработной плате и иных доходах, сведения о воинском учете, семейном положении, составе семьи, место работы или учебы членов семьи и родственников, сведения страховых полисов обязательного и (или) добровольного медицинского страхования, социальных льготах, идентификационный номер налогоплательщика, а также иная информация, необходимая для достижения вышеуказанных целей и предусмотренная действующим трудовым законодательством Российской Федерации;

– объем и содержание персональных данных физических лиц, состоявших или состоящих в договорных и иных отношениях с ОАО «Иркутскэнерго»: фамилия, имя, отчество, дата и место рождения, пол, гражданство, паспортные данные или данные иного документа удостоверяющего личность (серия, номер, когда и кем выдан), адрес места жительства, контактная информация, сведения о платежах за потребленные энергоресурсы, воинском учете, идентификационный номер налогоплательщика, а также иная информация, необходимая для достижения вышеуказанных целей.

5.5. При заключении трудового договора работник предъявляет в отдел по управлению персоналом ОАО «Иркутскэнерго» следующие документы (ст.65 ТК РФ):

- паспорт;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документ об образовании, о квалификации или наличии специальных знаний;
- документы воинского учета.

5.5.1 Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым кодексом, иными федеральными законами.

5.6. Сроки обработки персональных данных

5.6.1 Сроки обработки персональных данных определяются в соответствие со сроками действия договоров с субъектами персональных данных, а также требованиями законодательства и локальными документами ОАО «Иркутскэнерго».

5.7. Необходимость согласия субъекта на обработку персональных данных

5.7.1 В случаях, предусмотренных федеральным законом «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 в соответствии с федеральным законом электронной подписью.

5.7.2 При необходимости для каждой из категорий субъектов персональных данных разрабатывается и утверждается форма согласия на обработку персональных данных.

5.7.3 Для получения письменного согласия третьей стороной от имени ОАО «Иркутскэнерго» (на основании договора между ОАО «Иркутскэнерго» и третьей стороной)

разрабатывается форма такого согласия ОАО «Иркутскэнерго» и включается в договор с третьей стороной.

5.7.4 Формы согласий разрабатываются в соответствии с требованиями Федерального закона «О персональных данных». Примерные формы согласий приведены в Приложении 1.

6. Условия обработки персональных данных

6.1. Конфиденциальность персональных данных

6.1.1 В соответствии с Указом Президента Российской Федерации от 06.03.1997 г. №188 «Об утверждении перечня сведений конфиденциального характера», персональные данные относятся к сведениям конфиденциального характера.

6.1.2 В ОАО «Иркутскэнерго» на этапе создания или в ходе эксплуатации информационных систем производится инвентаризация информационных активов, и определение владельцами активов содержащих персональные данные, а затем документальное оформление и утверждение их для обработки в информационных системах.

6.1.3 Отнесение информационных систем обрабатывающих персональные данные к ИСПДн производится Актом классификации ИСПДн и утверждается председателем комитета по управлению информационной безопасностью. Далее владельцем ИСПДн назначается ответственный за обработку персональных данных.

6.1.4 При обработке персональных данных ОАО «Иркутскэнерго» и третьими лицами, получающими доступ к персональным данным, обеспечивается их конфиденциальность, т.е. создаются условия, не допускающие раскрытия и распространения персональных данных без согласия субъекта персональных данных, за исключением следующих случаев: в отношении общедоступных персональных данных.

6.2. Поручение обработки персональных данных третьему лицу

6.2.1 ОАО «Иркутскэнерго» вправе поручить обработку персональных данных третьему лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

6.2.2 Передача или поручение обработки персональных данных может выполняться на основе федерального закона, в этом случае согласие субъекта персональных данных не требуется.

6.2.3 В случае, если ОАО «Иркутскэнерго» на основании договора поручает обработку персональных данных третьему лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

6.2.4 Лицо, осуществляющее обработку персональных данных по поручению ОАО «Иркутскэнерго», обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных» и локальными документами ОАО «Иркутскэнерго».

6.2.5 Сведения о работающем или уволенном работнике могут быть предоставлены другой организации, физическим лицам или третьим лицам только по их письменному обращению с согласия работника.

6.3. Хранение и уничтожение персональных данных

6.3.1 Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

6.3.2 ОАО «Иркутскэнерго» прекращает обработку персональных данных и уничтожает собранные персональные данные, если иное не установлено законодательством РФ, в следующих случаях и в сроки, установленные законодательством РФ:

– по достижении целей обработки или утрате необходимости в их достижении;

– по требованию субъекта персональных данных или Уполномоченного органа по защите прав субъектов персональных данных - если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такой согласие требуется в соответствии с законодательством РФ;

– при невозможности устранения допущенных нарушений при обработке персональных данных.

6.4. Обработка персональных данных в целях продвижения товаров и услуг

6.4.1 Обработка персональных данных в целях продвижения товаров и услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, допускается только при условии предварительного согласия субъекта персональных данных, разработанного и утвержденного в соответствии с требованиями настоящего стандарта.

6.5. Трансграничная передача персональных данных

6.5.1 Трансграничная передача персональных данных (передача через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства) может осуществляться только при наличии письменного согласия субъекта персональных данных.

6.5.2 Трансграничная передача персональных данных может осуществляться без согласия субъекта персональных данных в случаях:

– исполнения договора, стороной которого является субъект персональных данных.

– защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

6.6. Обработка обращений и запросов

6.6.1 Порядок обработки обращений субъектов персональных данных (или их законных представителей) по вопросам обработки их персональных данных определен статьей 20 Федерального закона «О персональных данных».

7. Мероприятия по обеспечению безопасности персональных данных

7.1. Общие положения

7.1.1 Под угрозой для персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление возможностей внешних или внутренних злоумышленников или неблагоприятных событий, которые оказывают дестабилизирующее воздействие на защищаемую информацию.

7.1.2 Мероприятия по обеспечению безопасности персональных данных являются составной частью деятельности ОАО «Иркутскэнерго» и определяются на основании моделей угроз.

7.1.3 Для приведения деятельности ОАО «Иркутскэнерго» в соответствие с требованиями Федерального закона «О персональных данных» формируется Комитет по управлению информационной безопасностью ОАО «Иркутскэнерго», в состав которого включаются руководители структурных подразделений, отвечающие за отдельные направления работ в рамках обеспечения безопасности персональных данных в соответствии с СТП 011.473.140-2011 Система управления информационной безопасностью.

7.1.4 Для выбора и реализации методов и способов защиты персональных данных

могут привлекаться организации, имеющие оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

7.1.5 Порядок формирования списка лиц, доступ которых к персональным данным, обрабатываемым в информационных системах ОАО «Иркутскэнерго», необходим им для выполнения должностных обязанностей, определяется в СТП 011.473.134-2010 «Управление доступом к информационным ресурсам информационных систем».

7.1.6 Лица, допущенные к работе с персональными данными в информационных системах персональных данных, фиксируются в журнале учета запросов на предоставления доступа к персональным данным (Приложение 2).

7.1.7 Допускается указание работников в списке на ролевой основе. Роли задаются в соответствии с занимаемой должностью на основании требований:

– роли работников выделяются и документально определяются;

– роли персонифицируются с установлением ответственности за их выполнение, ответственность фиксируется в должностных инструкциях.

7.1.8 С целью снижения рисков нарушения информационной безопасности в рамках одной роли не совмещаются следующие функции: разработки и сопровождения системы/программного обеспечения, их разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора информационной безопасности, выполнения операций в системе и контроля их выполнения.

7.1.9 Документально процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющими получить контроль над защищаемым информационным активом ОАО «Иркутскэнерго» определены в СТП 011.473.152-2011 Аудит информационной безопасности.

7.1.10 Процедуры (которые предусматривают документальную фиксацию результатов проводимых проверок) приема на работу, влияющие на обеспечение информационной безопасности, включающие:

- проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов;

- проверку в части профессиональных навыков и оценку профессиональной пригодности

определены в соответствии с СТП 011.105.128-2010, СТП 001.042.100-2007, СТП 00.04.01.089.001-2003 ОАО «Иркутскэнерго».

7.1.11 Процедуры регулярной проверки (с документальной фиксацией результатов) в части профессиональных навыков и оценки профессиональной пригодности работников, а также внеплановой проверки (с документальной фиксацией результатов) - при выявлении фактов их нештатного поведения, участия в инцидентах информационной безопасности или подозрений в таком поведении или участии определены в соответствии с СТП 001.089.036-2006, СТП 001.042.100-2007 ОАО «Иркутскэнерго».

7.1.12 В соответствии с СТП 001.107.097-2008 при обработке конфиденциальной информации работники ОАО «Иркутскэнерго» дают письменное обязательство о неразглашении информации, включая приверженность правилам корпоративной этики и требования по недопущению конфликта интересов, этим каждый работник подтверждает, что он проинформирован о факте обработки им персональных данных, категориях обрабатываемых персональных данных, а также ознакомлен со всей совокупностью требований по обработке и обеспечению безопасности персональных данных, указанных в настоящем стандарте и иных внутренних нормативных документах, регламентирующих обработку персональных данных, в части, касающейся его должностных обязанностей.

7.1.13 При взаимодействии с организациями и физическими лицами требования по обеспечению информационной безопасности включаются в договоры (соглашения) с ними и регламентируют деятельность в этой области.

7.1.14 Обязанности работников по выполнению требований по обеспечению ИБ должны включаться в трудовые контракты (соглашения, договоры) и (или) должностные инструкции.

7.1.15 Перечень (список) лиц, имеющих доступ к персональным данным, обрабатываемым в информационных системах ОАО «Иркутскэнерго» может существовать в электронном виде или бумажном виде на основании распорядительного документа в документально зафиксированном в ОАО «Иркутскэнерго» порядке, при условии предоставления работникам прав доступа в информационные системы персональных данных.

7.1.16 Доступ работников ОАО «Иркутскэнерго» к персональным данным и обработка персональных данных работниками ОАО «Иркутскэнерго» осуществляется только для выполнения ими должностных обязанностей.

7.1.17 В ОАО «Иркутскэнерго» порядок доступа работников и иных лиц в помещения, в которых ведется обработка персональных данных определен СТП 011.534.043-2012 «О пропускном и внутриобъектовом режиме».

7.2. Мероприятия по обеспечению безопасности персональных данных при автоматизированной обработке

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

7.2.2 Все информационные системы персональных данных ОАО «Иркутскэнерго» подлежат обязательной классификации.

7.2.3 Классификация информационных систем персональных данных осуществляется ОАО «Иркутскэнерго» в соответствии с:

– порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 года 55/86/20;

– методикой определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн, утвержденной ФСТЭК России 14 февраля 2008 г.;

– стандартами и рекомендациями Минэнерго России по обеспечению информационной безопасности организаций топливно-энергетического комплекса Российской Федерации.

7.2.4 Процедура классификации информационных систем персональных данных включает в себя следующие этапы:

- перед началом обработки в ИСПДн любой категории персональных данных или во время инвентаризации владелец устанавливает их перечень (категорию) и объем (Приложение 4), вносит их в Акт классификации ИСПДн (Приложение 5; пункты 1,2) и направляет менеджеру системы ИБ;
- менеджер системы ИБ, используя Приложение 4, определяет класс ИСПДн, вносит его в Акт классификации ИСПДн (Приложение 5; пункт 3);
- менеджер системы ИБ направляет Акт классификации ИСПДн в управление по информационным технологиям для заполнения технической информации;
- управление по информационным технологиям заполняет Акт классификации ИСПДн (Приложение 5; пункты 4-8) и направляет менеджеру системы ИБ для актуализации;
- менеджер системы ИБ выносит Акт классификации ИСПДн для его рассмотрения и утверждения на Комитете по управлению информационной безопасностью;
- по результатам рассмотрения Комитет по управлению информационной безопасностью принимает решение о его утверждении или доработке;
- копия Акта классификации ИСПДн возвращается владельцу для хранения.

7.2.5 При отнесении информационных систем ОАО «Иркутскэнерго» к

информационным системам персональных данных используется следующий подход:

– информационные системы целью создания и использования, которых, в том числе, является обработка персональных данных, должны быть включены в список информационных систем, в которых обрабатываются персональные данные;

– информационные системы, реализующие бизнес процессы ОАО «Иркутскэнерго», не обрабатывающие персональные данные или отнесенные к 4 классу, не включаются в список ИСПДн.

7.2.6 Для каждой информационной системы персональных данных ответственным за обработку персональных данных подготавливаются сведения о:

– владельце информационной системы персональных данных;
– цели обработки персональных данных;
– объеме и содержании обрабатываемых персональных данных;
– перечне действий с персональными данными и способы их обработки.

7.2.7 Объем и содержание персональных данных, а также перечень действий и способы обработки персональных данных должны соответствовать целям обработки. В том случае, если для выполнения бизнес процесса, реализацию которого поддерживает информационная система, нет необходимости в обработке определенных персональных данных или дополнительных сведений, тогда они должны быть удалены.

7.3. Мероприятия по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации

7.3.1 При обработке в ОАО «Иркутскэнерго» персональных данных на бумажных носителях, в частности, при использовании типовых форм документов, характер информации, в которых предполагает или допускает включение в них персональных данных, должны соблюдаться требования, установленные Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановление Правительства РФ от 15.09.2008 г. №687.

7.3.2 Обработка персональных данных, без использования средств автоматизации, осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

7.3.3 Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

7.3.4 При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

7.3.5 Допускается передача материальных носителей персональных данных на хранение сторонней организации на основании договора, при этом, существенным условием договора является обязанность обеспечения указанной организацией конфиденциальности персональных данных и безопасности персональных данных при их обработке (хранении).

7.3.6 Работники ОАО «Иркутскэнерго», осуществляющие обработку персональных данных без использования средств автоматизации, информируются о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

7.3.7 Внутренними организационно-распорядительными документами ОАО «Иркутскэнерго» определяются места хранения персональных данных, обрабатываемых без использования средств автоматизации.

7.3.8 Материальные носители персональных данных, по достижении целей обработки содержащихся на них персональных данных, подлежат уничтожению, если иное не предусмотрено законодательством РФ (полное физическое и не восстановимое уничтожение ПДн, содержащихся на таких носителях).

7.3.9 Личные дела могут выдаваться на рабочие места только генеральному директору, в исключительных случаях, по письменному разрешению генерального директора, руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

7.4. Мероприятия по обеспечению безопасности персональных данных при хранении носителей персональных данных

7.4.1 В ОАО «Иркутскэнерго» определен порядок учета и хранения материальных носителей персональных данных устанавливающий:

– места хранения материальных носителей персональных данных;

– требования по обеспечению безопасности персональных данных при хранении их носителей;

– ответственных за реализацию требований по обеспечению безопасности персональных данных;

– порядок контроля выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных.

7.5. Подготовка частной модели угроз ИСПДн

7.5.1 Если по результатам исполнения п.7.2.7 система остается ИСПДн, то менеджером системы ИБ подготавливается Частная модель угроз ИСПДн, и выполняются следующие шаги:

- владелец ИСПДн вносит данные п.7.2.6 в Частную модель угроз ИСПДн (Приложение 6; пункты 4.1-4.4) и направляет менеджеру системы ИБ;
- менеджер системы ИБ направляет Частную модель угроз ИСПДн в управление по информационным технологиям для заполнения технической информации;
- управление по информационным технологиям заполняет Частную модель угроз ИСПДн (Приложение 6; пункты 4.5-4.11; Таблица 2) и направляет менеджеру системы ИБ;
- менеджер системы ИБ предоставляет Частную модель угроз ИСПДн экспертной комиссии в составе которой должны быть представители владельца ИСПДн, подразделения информационных технологий, службы безопасности и менеджер системы ИБ для экспертной оценки угроз информационной безопасности;
- экспертная комиссия уточняет перечень угроз и определяет возможность реализации угроз и опасность каждой угрозы, эти данные вносятся менеджером системы ИБ в Частную модель угроз ИСПДн;
- по окончании работы экспертной комиссии менеджер системы ИБ рассчитывает показатели и определяет актуальные угрозы безопасности ПДн;
- менеджер системы ИБ выносит на рассмотрение Комитета по управлению информационной безопасностью окончательный вариант Частной модели угроз ИСПДн, по результатам рассмотрения принимается решение о ее утверждении или доработке;
- копия Частной модели угроз ИСПДн возвращается владельцу ИСПДн для хранения.

7.6. Подготовка плана мероприятий по обеспечению безопасности ИСПДн

7.6.1 Менеджер системы ИБ совместно со службой безопасности подготавливает план мероприятий по обеспечению безопасности ИСПДн с указанием ответственных за мероприятия исполнителей, в соответствии с Политикой в области информационной безопасности ОАО "Иркутскэнерго" и рекомендациями положения «О методах и способах защиты информации в информационных системах персональных данных», утвержденного Приказом Федеральной службы по техническому и экспортному контролю 05.02.2010 г. №58, направляет его владельцу ИСПДн и ответственным за мероприятия на согласование.

7.6.2 Владелец ИСПДн и ответственные за мероприятия направляют согласованный план мероприятий по обеспечению безопасности ИСПДн менеджеру системы ИБ для

утверждения на комитете по управлению ИБ.

7.6.3 Менеджер системы ИБ направляет утвержденный план мероприятий по обеспечению безопасности ИСПДн владельцу ИСПДн.

7.6.4 В рамках исполнения требований информационной безопасности владелец ИСПДн выпускает приказ о назначении ответственных за обработку персональных данных и направляет утвержденный план мероприятий по обеспечению безопасности ответственным за мероприятия исполнителям.

7.6.5 Ответственные за мероприятия исполнители присылают отчеты о выполнении мероприятий владельцу ИСПДн.

7.6.6 Владелец ИСПДн после получения отчетов по всем мероприятиям плана направляет их менеджеру системы ИБ для рассмотрения на комитете по управлению ИБ.

7.6.7 Комитет по управлению ИБ при участии владельца ИСПДн или его представителя рассматривает отчеты представленные ответственными за мероприятия и оценивает степень соответствия мер защиты ПДн заданным требованиям информационной безопасности.

7.6.8 Менеджер системы ИБ готовит протокол с выводом комитета по управлению ИБ о степени соответствия мер защиты ПДн заданным требованиям по безопасности и направляет его владельцу ИСПДн.

7.6.9 Владелец ИСПДн готовит декларацию о соответствии ИСПДн в форме Акта соответствия (Приложение 7).

7.6.10 После декларирования ИСПДн все изменения в ней проходят процедуру согласования в установленном порядке.

8. Подразделения, осуществляющие функции по организации защиты персональных данных

8.1.1 В своей деятельности подразделения, осуществляющие функции по организации защиты персональных данных, руководствуются нормативно-правовыми актами Российской Федерации в области защиты персональных данных, настоящим стандартом и иными локальными актами ОАО «Иркутскэнерго».

8.1.2 Организация защиты персональных данных координируется Комитетом по управлению информационной безопасностью согласно СТП 011.473.140-2011.

8.1.3 Ответственный за обработку персональных данных назначается владельцем информационной системы персональных данных, посредством издания приказа.

8.1.4 Функции ответственного за обработку персональных данных:

– осуществление внутреннего контроля за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– доведение до сведения работников законодательства Российской Федерации о персональных данных, локальных нормативных документов по вопросам обработки персональных данных, требований к защите персональных данных;

– организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов;

– ведение журнала нештатных ситуаций (Приложение 3), внесение в него соответствующих записей в случае обнаружения фактов: несоблюдения условий хранения носителей персональных данных; использования средств обработки информации, которое может привести к нарушению конфиденциальности персональных данных или другим нарушениям.

8.2. Права подразделений, осуществляющих функции по организации защиты персональных данных

8.2.1 Подразделения, осуществляющие функции по организации защиты персональных данных, имеют право на:

– Запрос и получение необходимых материалов для организации и проведения работ по вопросам обеспечения безопасности персональных данных в ОАО «Иркутскэнерго».

– Привлечение к проведению работ по защите персональных данных других подразделений ОАО «Иркутскэнерго».

– Привлечение к проведению работ по защите персональных данных на договорной основе сторонних организаций.

– Контроль деятельности структурных подразделений ОАО «Иркутскэнерго», в части выполнения ими требований по обеспечению безопасности персональных данных.

8.3. Ответственность работников подразделений, осуществляющих функции по организации защиты персональных данных

8.3.1 Работники подразделений, осуществляющие функции по организации защиты персональных данных, несут ответственность за:

– Правильность и адекватность принимаемых решений по защите персональных данных.

– Качество проводимых работ и выполнение возложенных на него функций, предусмотренных настоящим стандартом.

9. Права и обязанности работников ОАО «Иркутскэнерго»

9.1.1 Права работника, регламентирующие защиту его персональных данных, установлены действующим законодательством Российской Федерации.

9.1.2 В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

- на сохранение и защиту своей личной и семейной тайны;
- исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- ознакомление с персональными данными оценочного характера, дополненное заявлением, выражающим его собственную точку зрения;
- определение своих представителей, подтвержденное доверенностью, для защиты своих персональных данных.

9.1.3 Работник обязан:

- передавать работодателю или его представителю комплект достоверных, документированных персональных данных;
- своевременно сообщать работодателю об изменении своих персональных данных.

9.1.4 Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

10.Контроль за выполнением требований

10.1. Контроль выполнения требований настоящего стандарта устанавливается в соответствии с порядком, установленным СТП 011.473.152-2011.

10.2. Для проверки выполнения требований стандарта приказом ОАО «Иркутскэнерго» могут быть созданы соответствующие комиссии.

10.3. Результаты проведенного контроля оформляются в виде заключения комиссии по проверке выполнения требований защиты персональных данных.

10.4. Мероприятия по контролю могут осуществляться на договорной основе сторонними организациями.

11.Ответственность

11.1. Ответственность за осуществление контроля выполнения требований настоящего стандарта, предоставление рекомендаций по их выполнению, а также за поддержание данного документа в актуальном состоянии несет Менеджер системы ИБ и руководитель ГЗИ.

11.2. Работники ОАО «Иркутскэнерго» в соответствии со своими должностными обязанностями, осуществляющие обработку персональных данных, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования персональных данных.

11.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, уголовную ответственность в соответствии с действующим законодательством.

11.4. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы с персональными данными работодатель вправе применить, предусмотренные Трудовым кодексом РФ дисциплинарные взыскания.

Приложение 1

Согласие субъекта на обработку персональных данных (примерная форма для работников)

ОАО «Иркутскэнерго»
Директору по работе с персоналом
В.Н.Корневу
от работника ОАО «Иркутскэнерго»
_____
(ФИО)
Адрес:_____,

Имеющий паспорт:_____

СОГЛАСИЕ
на обработку персональных данных

Я, _____,
(фамилия, имя, отчество полностью)
занимающий (ая) должность _____,
(наименование должности)
в подразделении _____,

даю согласие

Иркутскому открытому акционерному обществу энергетики и электрификации (ОАО «Иркутскэнерго»), 664025, г.Иркутск, ул. Сухэ-Батора, 3, на автоматизированную, в том числе в информационно-телекоммуникационных сетях, а также без использования средств автоматизации обработку, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение моих персональных данных: (фамилия, имя, отчество, год, месяц, дата и место рождения, гражданство, адрес места жительства, семейное положение и состав семьи, место работы или учебы членов семьи и родственников; номер телефона; образование, знание иностранных языков, профессия, предыдущий опыт работы, стаж работы, сведения, включенные в трудовую книжку; паспортные данные, сведения о воинском учете, сведения о наградах и почетных званиях, сведения о социальных льготах, идентификационный номер налогоплательщика, номер страхового свидетельства обязательного пенсионного страхования, заработная плата), в целях:

- обеспечения соблюдения законодательства Российской Федерации;
- содействия в трудоустройстве;
- содействия в обучении;
- оформления безналичного счета для перечисления заработной платы;
- для реализации программ добровольного медицинского страхования;
- оформления и приобретения авиа- и железнодорожных билетов;
- оформления визитных карточек;
- оформления участия в корпоративных пенсионных программах;
- оформления доверенностей на представление интересов ОАО «Иркутскэнерго»;
- содействия в продвижении по службе;
- формирования электронных справочников и электронных баз данных, необходимых ОАО «Иркутскэнерго», как работодателю, в связи с трудовыми отношениями.

Также даю согласие на:

- публичное обращение в мой адрес с использованием персональных данных (фамилия, имя, отчество, дата рождения) при: поздравлении с днем рождения; размещении на Доске почета; награждении за трудовые достижения, в том числе через публикацию в средствах массовой информации;
- включение моих персональных данных (фамилия, имя, отчество) в общедоступные источники: телефонный справочник ОАО «Иркутскэнерго», книга электронных адресов ОАО «Иркутскэнерго».

Настоящее согласие действует с момента его подписания в течение срока трудового договора с ОАО «Иркутскэнерго» и в течение 75 лет после его расторжения, и может быть отозвано путем подачи письменного заявления.

_____/_____/ __ __ 20__г.
(подпись) (расшифровка подписи)

Согласие субъекта на обработку персональных данных (примерная форма для других физических лиц)

СОГЛАСИЕ

на обработку персональных данных

Я , _____

(фамилия, имя, отчество)

проживающий (ая): _____

(адрес субъекта персональных данных)

Документ, удостоверяющий личность: _____

(номер, кем и когда выдан)

даю свое согласие оператору персональных данных - ОАО «Иркутскэнерго», (далее - Компания), расположенному по адресу: 664025, Россия, г. Иркутск, ул. Сухэ-Батора, д. 3 на обработку моих персональных данных в целях _____.

Действие согласия распространяется на следующую информацию, относящуюся к моим персональным данным: _____.

Настоящее согласие предоставляется на совершение любых действий (операций) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу определенному кругу третьих лиц для достижения вышеуказанных целей), обезличивание, блокирование, уничтожение, осуществляемых как с использованием средств автоматизации (автоматизированная обработка), так и без использования таких средств (неавтоматизированная обработка).

Настоящее согласие действует не менее _____ лет, в случае если иное не предусмотрено законодательством Российской Федерации.

Я уведомлен (а), что вправе отозвать согласие на обработку своих персональных данных путем направления мною соответствующего письменного запроса на почтовый адрес Компании.

В случае уточнения (обновления, изменения) моих персональных данных, я обязуюсь уведомить Компанию о таких уточнениях, путем направления мною соответствующего письменного уведомления на почтовый адрес Компании, не позднее _____ дней с момента уточнения. В случае если сведения об уточнении (обновлении, изменении) моих персональных данных были получены от третьих лиц, то Компания вправе не уведомлять меня об этом.

_____ _____ _____

(дата) (подпись) (фамилия и инициалы)

Приложение 2

Журнал учета запросов на предоставления доступа к персональным данным

№	Должность и подразделение	ФИО	Цель доступа	Категории персональных данных	Права доступа	Срок доступа	Примечания
1	2	3	4	5	6	7	8

Приложение 3

Журнал учета нештатных ситуаций (типовая форма)

Журнал учета нештатных ситуаций

№	Дата	Краткое описание нештатной ситуации*	Действие персонала	Заключение по фактам возникновения нештатной ситуации	ФИО, подпись ответственных лиц за действия персонала	ФИО, подпись ответственного за обработку персональных данных	Примечание
1	2	3	4	5	6	7	8

* - факты несоблюдения условий хранения носителей персональных данных, использования средств обработки информации, которые могут привести к нарушению конфиденциальности, целостности, доступности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных

Приложение 4.

Подготовка акта классификации ИСПДн.
(перечень (категория) и объем персональных данных)

1. Классификация информационных систем проводится на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

2. Проведение классификации информационных систем включает в себя следующие этапы:

- сбор и анализ исходных данных по информационной системе;
- присвоение информационной системе соответствующего класса и его документальное оформление.

3. При проведении классификации информационной системы учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных – $X_{ПД}$;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) – $X_{НПД}$;
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- структура информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы.

4. Определяются следующие категории обрабатываемых в информационной системе персональных данных ($X_{ПД}$):

категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;

категория 4 – обезличенные и (или) общедоступные персональные данные.

5. $X_{НПД}$ может принимать следующие значения:

1 – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 – в информационной системе одновременно обрабатываются персональные данные от 1 000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 – в информационной системе одновременно обрабатываются данные менее чем 1 000

субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

6. По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы – информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

7. К специальным информационным системам должны быть отнесены:

- информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;
- информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

8. По структуре информационные системы подразделяются:

- на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);
- на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);
- на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

9. По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

10. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

11. По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

12. Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

13. По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:

класс 1 (К1) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

класс 2 (К2) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

класс 3 (К3) – информационные системы, для которых нарушение заданной

характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

класс 4 (К4) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

14. Класс типовой информационной системы определяется в соответствии с таблицей.

$X_{ПД}$ \ $X_{НПД}$	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Приложение 5.

Акт классификации ИСПДн (примерная форма).

УТВЕРЖДАЮ
Председатель комитета по управлению
информационной безопасностью
ОАО «Иркутскэнерго»

« ____ » _____ 201_ г.

А К Т
классификации информационной системы персональных данных
«Наименование ИСПДн»

Комиссия в составе:
Председатель:
членыкомиссии:
рассмотрев следующие исходные данные на информационную систему персональных данных:

1. Категория обрабатываемых персональных данных (Хпд). Хпд = 1/2/3/4.

Обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
Обрабатываются персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.
Обрабатываются персональные данные, позволяющие идентифицировать субъекта персональных данных.
Обрабатываются обезличенные и (или) общедоступные персональные данные.

2. Объем обрабатываемых персональных данных (Хнпд). Хнпд = 3/2/1.

Одновременно обрабатываются данные менее чем 1000 субъектов персональных данных/Одновременно обрабатываются данные субъектов ПДн в объеме одной организации.
Одновременно обрабатываются данные от 1000 до 100000 субъектов персональных данных/Одновременно обрабатываются данные субъектов ПДн в объеме одной отрасли/органа власти/муниципального образования.
Одновременно обрабатываются данные более 100000 субъектов персональных данных/Одновременно обрабатываются данные субъектов ПДн в объеме РФ/субъекта РФ.

3. Требуемые характеристики безопасности персональных данных. Типовая/Специальная ИСПДн. К1/2/3 (специальная)

Необходимо выполнить следующие характеристики безопасности персональных данных: конфиденциальность, защищенность от уничтожения, изменения, блокирования, иное. На основании этого информационная система относится к специальной/типовой информационно системе персональных данных. По значению последствий нарушения заданной характеристики безопасности для субъектов персональных данных соответствующая типовым ИСПДн класса К1/2/3.

4. Структура информационной системы. Автоматизированные рабочие места/ Локальная информационная система/Распределенная информационная система.

Используются автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных.

Используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа.

Используются комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа.

5. Подключение информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена. Не имеет/Имеет подключения к сетям международного информационного обмена.

6. Режим обработки персональных данных. Одно / Многопользовательский.

7. Разграничение доступа. С разграничением / Без разграничения прав доступа.

8. Местонахождение технических средств информационной системы. Все средства находятся в пределах Российской Федерации/Технические средства частично или целиком находятся за пределами Российской Федерации.

на основании Методики определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн, утвержденной ФСТЭК России 14 февраля 2008 г., и в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным совместным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20,

РЕШИЛА

Установить информационной системе «Наименование ИСПДн» Класс К1/2/3 (специальная), нарушение заданных характеристик безопасности персональных данных, обрабатываемых в ней, (не) может привести к (незначительным, значительным) негативным последствиям для субъектов персональных данных.

«_____»_____201_ г.

Председатель комиссии _____ _____

Члены комиссии

_____ _____

_____ _____

_____ _____

Приложение 6.

Частная модель угроз ИСПДн (примерная форма).

УТВЕРЖДАЮ
Председатель комитета по управлению
информационной безопасностью
ОАО «Иркутскэнерго»

« ____ » _____ 201_ г.

Частная модель угроз

безопасности персональных данных

в информационной системе персональных данных

«Наименование ИСПДн»

201_ г. Иркутск.

Оглавление

1. Сокращения

АРМ – автоматизированное рабочее место;

АС – автоматизированная система;

АВС – антивирусные средства;

ВП – выделенное помещение;

ВТСС – вспомогательные технические средства и системы;

ИСПДн – информационная система персональных данных;

КЗ – контролируемая зона;

МЭ – межсетевой экран;

НДВ – не декларированные возможности;

НСД – несанкционированный доступ;

ОС – операционная система;

ПДн – персональные данные;

ПМВ – программно-математическое воздействие;

ПО – программное обеспечение;

ПЭВМ – персональная электронно-вычислительная машина;

ПЭМИН – побочные электромагнитные излучения и наводки;

САЗ – система анализа защищенности;

СВТ – средства вычислительной техники;

СЗИ – средства защиты информации;

СЗПДн – система (подсистема) защиты персональных данных:

СОВ – система обнаружения вторжений;

СУБД – система управления базами данных;

УБПДн – угрозы безопасности персональным данным.

2. Термины и определения.

В настоящем документе используются следующие термины и их определения:

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ к информации - возможность получения информации и ее использования.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание е сторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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

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.

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

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (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).

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - код программы, преднамеренно внесенный программу с целью осуществить утечку, изменить, блокировать, уничтожать информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

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

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Общие положения.

Настоящая Частная модель угроз безопасности персональных данных (далее – Модель угроз), в информационной системе персональных данных «Полное наименование ИСПДн» (далее ИСПДн), разработана на основании следующих документов:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- «Положение об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных» (утв. постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781);
- Совместный приказ ФСТЭК/ФСБ/Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 14 февраля 2008 г.);
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.);
- Положение "О методах и способах защиты информации в информационных системах персональных данных", утвержденное Приказом Федеральной службы по техническому и экспортному контролю 05.02.2010 г. №58.

4. Исходные данные об ИСПДн.

4.1. Владелец ИСПДн.

Владельцем информационной системы персональных данных «Наименование ИСПДн» является заместитель генерального директора...

4.2. Цель обработки персональных данных

Регистрация сведений, необходимых для осуществления ОАО "Иркутскэнерго" уставной деятельности

4.3. Объем и содержание обрабатываемых в ИСПДн персональных данных.

В данной системе обрабатываются следующие персональные данные, подлежащие защите:

- фамилия, имя, отчество;

- серия и номер документа, удостоверяющего личность.

4.4. Перечень действий с персональными данными и способы их обработки.

Оператором совершаются сбор, запись, хранение, уточнение. Ведется смешанная обработка ПДн.

4.5. Условия расположения основных составляющих АС, обрабатывающих персональные данные.

4.5.1. Расположение основных составляющих АС.

ИСПДн является распределенной и состоит из следующих структурных единиц:

- Исполнительная дирекция (ИД);

- филиалы (Ф);

- дополнительные офисы (ДО).

Обработка информационных потоков ИСПДн осуществляется в ИД, расположенном по адресу: г. Иркутск, XXXX.

4.5.2. Границы контролируемых зон.

Контролируемыми зонами являются здания в которых располагаются структурные единицы.

4.6. Топология ИСПДн и конфигурация ее отдельных компонентов.

4.6.1. Топология ИСПДн.

Основными составляющими ИСПДн являются:

- центральный узел обработки данных;

- узел администрирования;

- автоматизированные рабочие места (АРМ) сотрудников.

4.7. Конфигурация отдельных компонентов ИСПДн.

4.7.1. Центральный узел обработки данных.

Центральный узел обработки данных представляет собой сервер HP, с установленной операционной системой Unix. Всего в информационной системе АС используется один центральный узел обработки данных, который расположен в ИД г.Иркутск.

4.7.2. Узел администрирования.

Узел администрирования АС представляет собой АРМ Администратора безопасности, с установленной операционной системой Windows XP.

4.7.3. АРМ сотрудников.

Основным оборудованием, участвующим в обработке персональных данных, являются АРМ сотрудников. С помощью этого оборудования осуществляется ввод персональных данных в ИСПДн.

АРМ сотрудников установлено в зданиях ИД, Ф и ДО.

4.8. Связи между основными компонентами ИСПДн.

4.8.1. Физические связи.

Структура информационного взаимодействия в ИСПДн реализована на основе собственной распределенной Сети передачи данных (далее – СПД), с подключением к сетям связи общего пользования и сетям международного информационного обмена, и имеет следующие физические связи:

- Оборудование АС подключено к локальным сетям филиалов и дополнительных офисов по выделенным каналам связи;

- филиалы и дополнительные офисы соединены общей сетью передачи данных;

- центральный узел обработки данных подключен с АС к сетям международного информационного обмена;

- узел администрирования подключен в локальную сеть ИД.

4.8.2. Технологические связи.

В процессе обработки персональных данных в ИСПДн используются следующие технологии:

- персональные данные хранятся на центральном узле обработки данных в специально предназначенной для этого СУБД;

- ПО, обеспечивающее передачу персональных данных от конечного периферийного оборудования до СУБД, работает по протоколу TCP/IP;

4.8.3. Функциональные связи.

Введенные на АРМ сотрудников данные пересылаются непосредственно на центральный узел обработки данных.

Узел администрирования осуществляет централизованное управление и конфигурацию того участка защищенной сети, в котором он расположен:

- дает доступ в защищенную сеть для АРМ сотрудников;

- устанавливает политики безопасности, в соответствии с которыми АРМ сотрудников получают возможность работать с центральным узлом обработки данных;

Структура ИСПДн и информационных потоков в ней приведена на схеме (см. Рисунок 1).

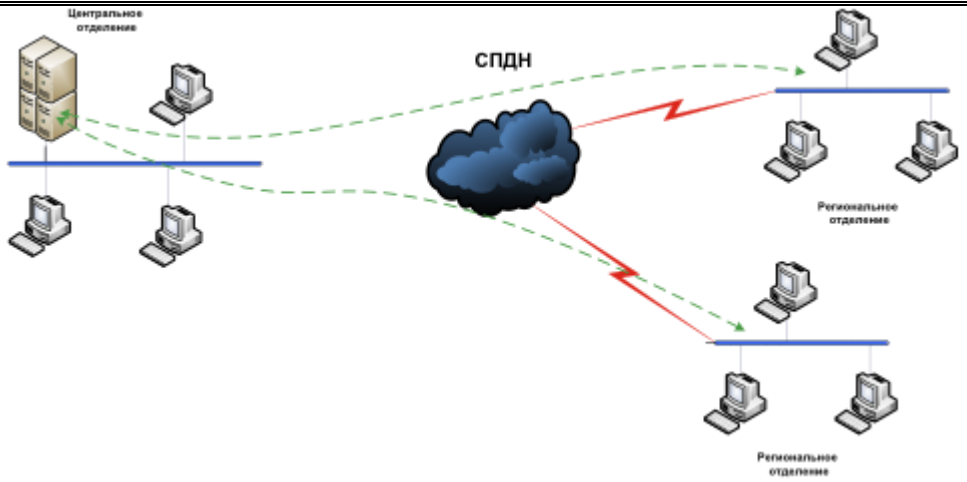


Рисунок 1. Схема ИСПДн и информационных потоков в ней.

4.9. Технические средства, участвующие в обработке персональных данных в ИСПДн.

В обработке персональных данных участвуют следующие технические средства:

- Сервера HP;

- АРМ сотрудников;

Кроме того, в обработке персональных данных участвует активное и пассивное сетевое оборудование производства Cisco: коммутаторы, межсетевые экраны, маршрутизаторы, модемы.

4.10. Общесистемные и прикладные программные средства, участвующие в обработке персональных данных.

В обработке персональных данных участвует следующее общесистемное программное обеспечение:

- ОС Unix;

- ОС Windows 2003/2008/XP/Vista/Windows7.

В обработке персональных данных участвует следующее прикладное программное обеспечение:

- ПО «Автоматизированная система v.1»;

- СУБД Oracle.

4.11. Режим и степень участия персонала в обработке персональных данных.

Обработка персональных данных во всех компонентах ИСПДн осуществляется в многопользовательском режиме.

4.11.1. Персонал, участвующий в обработке данных.

В процессе обработки персональных данных участвует следующий персонал:

- Администратор узла обработки данных осуществляет настройку отдельной серверной части, обрабатывающей данные от нескольких отделений;

- Администратор безопасности занимается обслуживанием и настройкой узла администрирования. Администраторы безопасности находятся в каждом из отделений;

- Администратор сети занимается обслуживанием и настройкой сетевого оборудования. Администраторы сети находятся в каждом отделении.

- Пользователь осуществляет ввод персональных данных в систему АС.

4.11.2. Полномочия персонала, участвующего в обработке данных.

Персонал, участвующий в обработке персональных данных, наделен следующими полномочиями:

- Администратор узла обработки данных осуществляет разграничение доступа конечного оборудования к базе, содержащей персональные данные.

- Администратор безопасности осуществляет разграничение доступа в защищенную инфраструктуру ИСПДн. Администратор безопасности не имеет полномочий настраивать центральный узел обработки данных.

- Администратор сети отвечает за настройку и бесперебойную работу сетевого оборудования. Администратор сети не имеет полномочий настраивать центральный узел обработки данных, сервер безопасности, а также устанавливать и разграничивать права доступа в защищенную инфраструктуру ИСПДн.

- Пользователь не имеет полномочий вносить модификации в настройки какого-либо оборудования и прикладного ПО. Кассир уполномочен вводить персональные данные в базу данных ИСПДн.

5. Расчет частной модели угроз безопасности персональных данных, обрабатываемых в ИСПДн.

При обработке ПДн в ИСПДн АС возможна реализация следующих УБПДн:

- угрозы утечки по техническим каналам;

- угрозы НСД к ПДн.

Угрозы утечки по техническим каналам включают в себя:

- угрозы утечки акустической (речевой) информации;

- угрозы утечки видовой информации;

- угрозы утечки по каналу ПЭМИН.

Угрозы НСД к ПДн в ИСПДн АС включают в себя:

- угрозы, реализуемые в ходе загрузки операционной системы, направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

- угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);

- угрозы внедрения вредоносных программ;

- угрозы "Анализ сетевого трафика" с перехватом передаваемой по сети информации;

- угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.

- угрозы типа "Отказ в обслуживании";

- угрозы выявления паролей;

- угрозы удаленного запуска приложений;

- угрозы внедрения ложного объекта сети;

- угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;

- угрозы внедрения по сети вредоносных программ.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн (внутренний нарушитель).

5.1. Определение уровня исходной защищенности ИСПДн.

Под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

Исходная степень защищенности определяется следующим образом.

1) (Y1=0). ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню "высокий" (суммируются положительные решения но первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2) (Y1=5). ИСПДн имеет средний уровень исходной защищенности, если не

выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний" (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3) (Y1=10). ИСПДн имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2.

Таблица 2. Характеристики ИСПДн, определяющие исходный уровень защищенности.

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
- распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	-	-	+
- городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	-	-	+
- корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	-	+	-
- локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	-	+	-
- локальная ИСПДн, развернутая в пределах одного здания.	+	-	-
2. По наличию соединения с сетями общего пользования:			
- ИСПДн, имеющая многоточечный выход в сеть общего пользования;	-	-	+
- ИСПДн, имеющая одноточечный выход в сеть общего пользования;	-	+	-
- ИСПДн, физически отделенная от сети общего пользования.	+	-	-
3. По встроенным (легальным) операциям с записями баз персональных данных:			
- чтение, поиск;	+	-	-
- запись, удаление, сортировка;	-	+	-
- модификация, передача.	-	-	+
4. По разграничению доступа к персональным данным:			
- ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	-
- ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	-	-	+
- ИСПДн с открытым доступом.	-	-	+
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
- интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	-	–	+
- ИСПДн, в которой используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн.	+	-	-
6. По уровню обобщения (обезличивания) ПДн:			
- ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	-	-

- ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	-	+	-
- ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн).	-	-	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
- ИСПДн, предоставляющая всю БД с ПДн;	-	-	+
- ИСПДн, предоставляющая часть ПДн;	-	+	-
- ИСПДн, не предоставляющие никакой информации.	+	-	-

В соответствии с таблицей 2, не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний", следовательно Y1=5.

5.2. Определение вероятности реализации угроз в ИСПДн

Под вероятностью реализации угрозы поднимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализации конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Вероятность (Y2) определяется по 4 вербальным градациям этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

- средняя вероятность – объектные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);

- высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

Оценка вероятности реализации угрозы безопасности различными категориями нарушителей (Kn) приведена в таблице 3/

Таблица 3

Угроза безопасности ПДн	Вероятность реализации угрозы нарушителем категории Kn									
	K0	K1	K2	K3	K4	K5	K6	K7	K8	Итог Y2
угрозы утечки акустической (речевой) информации	0	0	0	0	0	0	0	0	0	0
угрозы утечки видовой информации	2	0	0	0	2	5	2	0	0	5
угрозы утечки по каналу ПЭМИН	0	0	0	0	0	0	0	0	0	0
угрозы, реализуемые в ходе загрузки операционной системы	0	0	0	0	0	0	0	0	0	0

угрозы, реализуемые после загрузки операционной системы	0	2	2	2	2	2	2	2	2	2
угрозы внедрения вредоносных программ	2	2	0	0	5	2	5	5	5	5
угрозы "Анализ сетевого трафика" с перехватом передаваемой по сети информации	2	2	0	0	2	2	2	2	0	2
угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	2	2	0	0	2	2	2	2	0	2
угрозы типа "Отказ в обслуживании"	2	2	0	0	2	2	2	2	2	2
угрозы выявления паролей	2	2	0	0	2	0	0	0	0	2
угрозы удаленного запуска приложений	2	2	0	0	2	2	2	2	0	2
угрозы внедрения ложного объекта сети	2	2	2	2	2	2	2	2	0	2
угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	5	5	0	0	0	0	0	0	0	5
угрозы внедрения по сети вредоносных программ	2	2	0	0	2	2	2	2	0	2

5.3. Определение возможности реализации угрозы в ИСПДн АС

По итогам оценки уровня исходной защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы (Таблица 4). Коэффициент реализуемости угрозы рассчитывается по формуле: Y=(Y1+Y2)/20. При этом возможность реализации угрозы определяется по:

$0 \le Y \le 0,3$ - Низкая;

$0,3 < Y \le 0,6$ - Средняя;

$0,6 < Y \le 0,8$ - Высокая;

$Y > 0,8$ - Очень высокая.

Таблица 4

Угроза безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы
угрозы утечки акустической (речевой) информации	0,25	низкая
угрозы утечки видовой информации	0,5	средняя
угрозы утечки по каналу ПЭМИН	0,25	низкая
угрозы, реализуемые в ходе загрузки операционной системы	0,25	низкая
угрозы, реализуемые после загрузки операционной системы	0,35	средняя
угрозы внедрения вредоносных программ	0,5	средняя
угрозы "Анализ сетевого трафика" с перехватом передаваемой по сети информации	0,35	средняя

угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	0,35	средняя
угрозы типа "Отказ в обслуживании"	0,35	средняя
угрозы выявления паролей	0,35	средняя
угрозы удаленного запуска приложений	0,35	средняя
угрозы внедрения ложного объекта сети	0,35	средняя
угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	0,25	низкая
угрозы внедрения по сети вредоносных программ	0,35	средняя

5.4. Оценка опасности угроз в ИСПДн АС

Оценка опасности производится на основе опроса специалистов по защите информации, технических специалистов и владельцев ИСПДн, и определяется вербальным показателем опасности, который имеет 3 значения:

- низкая опасности – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

- средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности приведена в таблице 5.

Таблица 5

Угроза безопасности ПДн	Опасность угроз
угрозы утечки акустической (речевой) информации	низкая
угрозы утечки видовой информации	средняя
угрозы утечки по каналу ПЭМИН	низкая
угрозы, реализуемые в ходе загрузки операционной системы	низкая
угрозы, реализуемые после загрузки операционной системы	низкая
угрозы внедрения вредоносных программ	средняя
угрозы "Анализ сетевого трафика" с перехватом передаваемой по сети информации	средняя
угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	низкая
угрозы типа "Отказ в обслуживании"	низкая
угрозы выявления паролей	низкая
угрозы удаленного запуска приложений	низкая
угрозы внедрения ложного объекта сети	низкая
угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	средняя

угрозы внедрения по сети вредоносных программ	низкая

5.5. Перечень актуальных угроз безопасности ПДн в ИСПДн АС

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн АС существуют следующие актуальные угрозы (таблица 7). Отнесение угрозы к актуальной производится по правилам, приведенным в таблице 6.

Таблица 6

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Таблица 7

Наименование угрозы безопасности ПДн	Тип угрозы (потеря конфиденциальности, потеря целостности, потеря доступности)	Актуальность	
		Возможность реализации угрозы (низкая, средняя, высокая, очень высокая)	Показатель опасности (низкая средняя, высокая)
УГРОЗА 1	Нарушение целостности	АКТУАЛЬНАЯ	
		средняя	средний
УГРОЗА 2	Нарушение доступности	НЕАКТУАЛЬНАЯ	
		средняя	низкий
УГРОЗА 3	Потеря конфиденциальности	АКТУАЛЬНАЯ	
		высокая	средний

Таким образом, актуальными угрозами безопасности ПДн в ИСПДн являются:

- угрозы утечки видовой информации;

- угрозы внедрения вредоносных программ;

- угрозы "Анализ сетевого трафика" с перехватом передаваемой по сети информации.

Приложение 7.

Акт соответствия (примерная форма).

А К Т № _____ соответствия ИСПДн «Наименование ИСПДн» требованиям по обеспечению безопасности информации

Комиссия в составе:

Председатель:

члены комиссии:

рассмотрев следующие документы на ИСПДн «Наименование ИСПДн»:

1. Акт классификации ИСПДн от __.__._____ ;
2. Модель угроз ИСПДн от __.__._____ ;
3. Требования по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн указанные в плане мероприятий по обеспечению безопасности ИСПДн от __.__._____ № _____;
4. Протокол о степени соответствия мер защиты ПДн заданным требованиям по безопасности.

и проведя анализ существующих мер по обеспечению безопасности персональных данных в ИСПДн УСТАНОВИЛА что ИСПДн «Наименование ИСПДн» соответствует требованиям по обеспечению безопасности информации для класса ИСПДн К1/2/3 .

«_____»_____201 _ г.

Председатель комиссии	_____	_____
Члены комиссии		
	_____	_____
	_____	_____
	_____	_____

Лист регистрации изменений

Порядковый номер изменения	Основание[1]	Срок введения изменения	Изменения внёс			Примечания
			ФИО	Подпись	Дата внесения изменения	

[1] Ссылка на документ, разрешающий внесение изменений и содержащий тест изменений.