СТП 001.017.067-2016

Стандарт предприятия

О защите персональных данных

Взамен СТП 001.004.008-2013

УТВЕРЖДАЮ
И.о. Генерального директора
ОАО «ИЭСК»

_____ Ю.Н. Терских
_____ 21 марта 2017
(дата)

Наименование подразделения - разработчика: Группа по безопасности и режиму

Введен в действие приказом
ОАО «ИЭСК»
от 21.03.2017 № 06.001-01-2.1-0099/1

ОАО «ИЭСК»

Содержание

Введение

Настоящий Стандарт предприятия разработан взамен СТП 001.004.008-2013 в связи с переводом части функций из состава обеспечивающего процесса ОАО «ИЭСК» «Управление информационными технологиями» в аутсорсинг.

1. Область применения

1.1 Настоящий стандарт устанавливает общие требования к обеспечению безопасности персональных данных, обрабатываемых в ОАО «ИЭСК» (далее Общество) 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 распространяется на все подразделения Общества и рекомендован к адаптации и применению в ДЗО ОАО «ИЭСК». Работники Общества, осуществляющие обработку персональных данных, должны быть ознакомлены с настоящим стандартом.

1.3 Настоящий стандарт предприятия входит в состав нормативных документов системы управления Общества.

2. Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие документы:

- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
- Трудовой кодекс Российской Федерации;
- Указ Президента Российской Федерации от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера»;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 14.02.2008;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 15.02.2008;
- Постановление Правительства Российский Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российский Федерации от 15.09.2008 №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- СТП 001.017.062-2016 «Политика в области информационной безопасности»;
- СТП 001.017.063-2016 «Система управления информационной безопасностью»;
- СТП 001.017.064-2016 «Управление доступом к информационным ресурсам ИС»;
- СТП 001.017.066-2016 «Аудит информационной безопасности».

3. Сокращения и определения

3.1. В настоящем стандарте используются следующие сокращения:

АРМ – автоматизированное рабочее место;
АС – автоматизированная система;
АВС – антивирусные средства;
ВП – выделенное помещение;
ВТСС – вспомогательные технические средства и системы;
ГБР – группа по безопасности и режиму
ИБ - информационная безопасность;
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.

3.2. В настоящем стандарте используются следующие 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 обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

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

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;

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание 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;

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, систематиза-

цию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, сделанные общедоступными субъектом персональных данных, в том числе размещенные в общедоступных источниках.

Общедоступные источники персональных данных – общедоступные источники данных, в которые с письменного согласия субъекта персональных данных могут включаться персональные данные, сообщаемые субъектом персональных данных. общедоступные источники данных, в которые с письменного согласия субъекта персональных данных могут включаться персональные данные, сообщаемые субъектом 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;

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

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

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

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;

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 физио-

логически и биологические особенности человека, на основании которых можно установить его личность;

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;

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;

Соискатель/кандидат – физическое лицо, обратившееся в Общество с целью поиска работы, либо информация о котором получена из общедоступных источников.

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;

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);

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

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;

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.

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

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;

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

Подразделение ИБ – подразделение или должностное лицо Общества, которое функционально отвечает за обеспечение информационной безопасности либо компании, которые обеспечивают данную функцию по договору возмездного оказания услуг.

Служба ИТ – сотрудник (подразделение) Общества, осуществляющий функции ИТ обеспечения Общества, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.

4. Общие 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. Общество 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 Обществом 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 Общество производит уведомление уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных, согласно статье 22 Федерального закона от 27.07.2006 года №152-ФЗ «О персональных данных».

5. Субъекты и категории персональных данных, цели обработки

5.1. Категории субъектов персональных данных

5.1.1. В Обществе может осуществляться обработка персональных данных следующих категорий субъектов персональных данных:

- физические лица, состоящие или состоявшие в договорных и иных отношениях с Обществом;
- физические лица, состоящие или состоявшие в договорных и иных отношениях с организациями, которые поручили Обществу в соответствии с договором, обрабатывать персональные данные этих физических лиц;
- соискатели/кандидаты;
- работники, состоящие или состоявшие в трудовых отношениях с Обществом.

– физические лица, в отношении которых, в соответствии СТП 001.015.054-2016 «Порядок работы персонала ОАО «ИЭСК» по выявлению, фиксации, расчету и взысканию объема неучтенного (бездоговорного) потребления электрической энергии», составляются акты о неучтенном (бездоговорном) потреблении электрической энергии.

– физические лица, у которых производится замена счетчиков электроэнергии с оформлением соответствующего акта допуска прибора учета в эксплуатацию.

5.2. Категории персональных данных субъектов персональных данных

5.2.1. В Обществе 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, отнесенные в соответствии с Федеральным законом «О персональных данных» к обезличенным персональным данным или расположенные в общедоступных источниках;

–персональные данные, которые не могут быть отнесены к вышеуказанным категориям персональных данных.

5.2.2. В информационных системах Общества 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 Обществе только с его письменного согласия.

Обработка всех категорий персональных данных может осуществляться только в установленных законодательством случаях.

5.3. Цели обработки персональных данных

5.3.1. В Обществе определены следующие цели обработки персональных данных:

–обработка персональных данных работников Общества может осуществляться с целью организации учета работников Общества, 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 Общества;

–обработка персональных данных физических лиц, состоящих или состоявших в договорных и иных отношениях с организациями, которые поручили Обществу в соответствии с договором, может осуществляться с целью организации учета, страхования, продвижения по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, иными федеральными законами, а также локальными актами этих организаций;

–обработка персональных данных соискателей/кандидатов осуществляется с целью трудоустройства либо содействия в трудоустройстве с возможностью хранения персональных данных в течение срока, указанного в Согласии на обработку персональных данных;

–обработка персональных данных физических лиц, состоявших или состоящих в договорных и иных отношениях с Обществом, осуществляется с целью осуществления уставных видов деятельности.

–обработка персональных данных физических лиц, в отношении которых, в соответствии СТП 001.015.054-2016 «Порядок работы персонала ОАО «ИЭСК» по выявлению, фиксации, расчету и взысканию объема неучтенного (бездоговорного) потребления электрической энергии» составляются акты о неучтенном (бездоговорном) потреблении электрической энергии, с целью взыскания объема неучтенного (бездоговорного) потребления электрической энергии.

–обработка персональных данных физических лиц, у которых производится замена счетчиков электроэнергии с оформлением соответствующего акта допуска прибора учета в эксплуатацию, с целью соблюдения Постановления Правительства РФ от 06.05.2011 N 354

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 Общества: 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 регистрации, 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 (ИНН), страховое сведетельство государственного пенсионного страхования (СНИЛС), а также иная информация, необходимая для достижения вышеуказанных целей и предусмотренная действующим трудовым законодательством Российской Федерации;

–объем и содержание персональных данных физических лиц, состоящих или состоявших в договорных и иных отношениях с организациями, которые поручили Обществу в соответствии с договором обработку таких данных, определяется по согласованию сторон;

–объем и содержание персональных данных соискателей/кандидатов: фамилия, имя, отчество, возраст, пол, гражданство, 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, 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 Общества: фамилия, имя, отчество, дата и место рождения, пол, гражданство, паспортные данные или данные иного документа удостоверяющего личность (серия, номер, когда и кем выдан), адрес регистрации, адрес места жительства, контактная информация, информация о воинском учете, идентификационный но-

мер налогоплательщика, а также иная информация, необходимая для достижения вышеуказанных целей.

–объем и содержание персональных данных физических лиц, в отношении которых, в соответствии СТП 001.015.054-2016 «Порядок работы персонала ОАО «ИЭСК» по выявлению, фиксации, расчету и взысканию объема неучтенного (бездоговорного) потребления электрической энергии» составляются акты о неучтенном (бездоговорном) потреблении электрической энергии: фамилия, имя, отчество, дата и место рождения, паспортные данные или данные иного документа удостоверяющего личность (серия, номер, когда и кем выдан), адрес регистрации, адрес места жительства, номер телефона, а также иная информация, необходимая для достижения вышеуказанных целей.

объем и содержание персональных данных физических лиц, у которых производится замена счетчиков электроэнергии с оформлением соответствующего акта допуска прибора учета в эксплуатацию, с целью соблюдения Постановления Правительства РФ от 06.05.2011 N 354: фамилия, имя, отчество, дата и место рождения, паспортные данные или данные иного документа удостоверяющего личность (серия, номер, когда и кем выдан), адрес регистрации, адрес места жительства, номер телефона, а также иная информация, необходимая для достижения вышеуказанных целей.

5.5. **При заключении трудового договора работник предъявляет в Общество 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 (СНИЛС);
- документ об образовании, о квалификации или наличии специальных знаний, при поступлении на работу, требующую специальных знаний или специальной подготовки;
- документы воинского учета, для военнообязанных и лиц, подлежащих призыву на военную службу
- по желанию работника, он может предоставить справку «О сумме заработной платы, иных выплат и вознаграждений, на которую были начислены страховые взносы на обязательное социальное страхование на случай временной нетрудоспособности и в связи с материнством, за два календарных года, предшествующих году прекращения работы (службы, иной деятельности) или году обращения за справкой, и текущий календарный год»;
- в отдельных случаях с учетом Трудового кодекса, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

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 Общества.

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. 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 №188 «Об утверждении перечня сведений конфиденциального характера», персональные данные относятся к сведениям конфиденциального характера.

6.1.2. В Обществе 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 Обществом 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 общедоступных персональных данных.

6.2. Поручение обработки персональных данных третьему лицу

6.2.1. Общество 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 Общество 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 Общества, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных» и локальными документами Общества.

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. Общество 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 Общества и определяются на основании моделей угроз.

7.1.3. Для приведения деятельности Общества в соответствие с требованиями Федерального закона «О персональных данных» формируется Комитет по управлению информационной безопасностью, в состав которого включаются руководители структурных подразделений, отвечающие за отдельные направления работ в рамках обеспечения безопасности персональных данных в соответствии с СТП 001.017.063-2016 «Система управления информационной безопасностью».

7.1.4. Для выбора и реализации методов и способов защиты персональных данных привлекаются только 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, необходим им для выполнения должностных обязанностей, определяется в СТП 001.017.064-2016 «Управление доступом к информационным ресурсам ИС». Допускается указание работников в списке на ролевой основе. Роли задаются в соответствии с занимаемой должностью.

7.1.6. 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.

7.1.7. Документально процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющими получить контроль над защищаемым информационным активом определены в СТП 001.017.066-2016 «Аудит информационной безопасности».

7.1.8. 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;

7.1.9. При обработке конфиденциальной информации работники Общества 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.

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

7.1.11. Доступ работников Общества к персональным данным и обработка персональных данных работниками Общества осуществляется только для выполнения ими должностных обязанностей.

7.2. Определение уровня защищенности ИСПДн

7.2.1. Все информационные системы персональных данных Общества подлежат обязательной классификации.

7.2.2. Классификация информационных систем персональных данных осуществляется Обществом в соответствии с:

–методикой определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн, утвержденной ФСТЭК России 14.02.2008;

–Постановлением Правительства Российский Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

–Приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

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

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

- перед началом обработки в ИСПДн любых персональных данных или во время инвентаризации владелец устанавливает их категорию, объем и характеристики безопасности (Приложение 3), вносит их в Акт классификации ИСПДн (Приложение 4) и направляет в ГБР;

- работник ГБР и службы ИТ, используя Приложение 3, определяет уровень защищенности ИСПДн, вносит его в Акт классификации ИСПДн (Приложение 4);

- работник ГБР направляет Акт классификации ИСПДн руководителю службы ИТ. Руководитель службы ИТ назначает ответственного работника для заполнения технической информации в акте;

- работник службы ИТ заполняет Акт классификации ИСПДн (Приложение 4; пункты 4-8) и направляет работнику ГБР для актуализации;

- работник ГБР 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.

7.2.4. При отнесении информационных систем 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, не обрабатывающие персональные данные или отнесенные к 4 классу, не включаются в список ИСПДн.

7.2.5. 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.

7.2.6. 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 Обществе 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 Постановлением Правительства РФ от 15.09.2008 г. №687, а также положения внутренних нормативных документов Общества.

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 Общества, 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 Общества 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).

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

7.4.1. Порядок учета и хранения материальных носителей персональных данных в Обществе определяется приказом, который устанавливает:

−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 система остается ИСПДн, то ГБР подготавливается Частная модель угроз ИСПДн, и выполняются следующие шаги:

- владелец ИСПДн вносит данные п.7.2 в Частную модель угроз ИСПДн (Приложение 5; пункты 4.1-4.4) и направляет работнику ГБР;
- работник ГБР направляет Частную модель угроз ИСПДн руководителю Службы ИТ. Руководитель службы ИТ назначает ответственного работника для заполнения технической информации;
- работник службы ИТ заполняет Частную модель угроз ИСПДн (Приложение 5; пункты 4.5-4.11; Таблица 2) и направляет в ГБР;
- работник ГБР предоставляет Частную модель угроз ИСПДн экспертной комиссии в составе которой должны быть представители владельца ИСПДн, службы ИТ, ГБР для экспертной оценки угроз информационной безопасности;
- экспертная комиссия уточняет перечень угроз и определяет возможность реализации угроз и опасность каждой угрозы, эти данные вносятся работником службы ИТ в Частную модель угроз ИСПДн;
- по окончании работы экспертной комиссии работник службы ИТ рассчитывает показатели и определяет актуальные угрозы безопасности ПДн;
- работник службы ИТ и ГБР выносят 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. Службы ИТ и ГБР подготавливает план мероприятий по обеспечению безопасности ИСПДн с указанием ответственных за мероприятия исполнителей, в соответствии с Политикой в области информационной безопасности и приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», 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 в ГБР для утверждения на комитете по управлению ИБ.

7.6.3. Работник ГБР 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 в ГБР 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. Работник ГБР 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 6).

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. Организация защиты персональных данных координируется Комитетом по управлению информационной безопасностью согласно СТП 001.017.063-2016 «Система управления информационной безопасностью».

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

8.1.3. Функции ответственного за обработку персональных данных:

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

–доведение до сведения работников положений законодательства Российской Федерации о персональных данных, локальных актов 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 2), 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 работников подразделений, осуществляющих функции по организации защиты персональных данных

8.2.1. Работники, 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 Обществе;

–привлечение к проведению работ по защите персональных данных других подразделений Общества;

–привлечение к проведению работ по защите персональных данных на договорной основе сторонних организаций;

–контроль деятельности структурных подразделений Общества, 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 Общества

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.

10. Контроль выполнения требований данного стандарта

10.1. Контроль выполнения требований настоящего стандарта устанавливается в соответствии с порядком, установленным СТП 001.017.066-2016 «Аудит информационной безопасности».

10.2. Для проверки выполнения требований стандарта приказом Общества 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 несут работники ГБР.

11.2. Работники Общества 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.

Приложение № 1[1]

Исполняющему обязанности Генерального директора ОАО «ИЭСК» Терских Ю.Н.

от

_____

(Ф.И.О.)

Согласие на передачу и обработку персональных данных

Я, ***ФИО, паспорт (серия, номер, выдан), зарегистрированный по адресу (адрес регистрации)***, в соответствии с нормативными правовыми актами Российской Федерации, регулирующими вопросы защиты персональных данных работников, свободно, своей волей и в своем интересе даю согласие ***Открытому акционерному обществу «Иркутская электросетевая компания» (ОАО «ИЭСК»),*** далее – Оператор, адрес ***г. Иркутск, ул. Лермонтова, 257***: на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 статьи 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных",

в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения, исполнения, оформления и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления и выплаты заработной платы и иных платежей с использованием банковской карты;
- исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ;
- предоставления сведений в банк для оформления банковской карты и перечисления на нее заработной платы;
- предоставления сведений третьим лицам для оформления полиса ДМС;
- предоставления налоговых вычетов;
- обучения, повышения квалификации, переобучения, продвижения по службе;
- контроля количества и качества выполняемой мной работы;
- обеспечения сохранности моего имущества и Оператора;
- предоставления гарантий и льгот, предусмотренных нормативными правовыми актами, локальными нормативными актами, соглашениями, трудовым договором;
- включения в корпоративные справочники и другие общественно доступные источники информации Оператора (в том числе размещение информации на корпоративных интернет-ресурсах (сайтах));
- идентификации и аутентификации меня в информационных системах,
- публичное обращение, публичное поздравление с днем рождения, юбилеями;
- страхования жизни и здоровья;

[1] Изм.1 Приказ от 06.11.2018 №06.001-01-2.1-0583

- проведения статистических и иных исследований и опросов;
- создания и ведения информационных систем - "1С: Зарплата и управление персоналом".
- оформления и приобретения авиа- и железнодорожных билетов;
- оформления доверенностей на представление интересов ОАО «ИЭСК»;
- участия в корпоративных проектах развития персонала;
- проведения аттестации;
- формирования Плана преемственности и кадрового резерва;
- контроля прохождения через систему доступа (при наличии автоматизированной программы учета доступа) в здание, к месту работы;
- для ведения реестра аттестационных комиссий предприятий (Личные данные членов комиссий по проверке знаний норм и правил работы в электроустановках (Ф.И.О., сведения об образовании, № диплома и дата выдачи, дата последнего повышения квалификации по должности;
- для прохождения аттестации в Ростехнадзоре (согласно Приказа Ростехнадзора от 29.01.2007 N 37 (ред. от 27.08.2010) «О порядке подготовки и аттестации работников организаций, поднадзорных Федеральной службе по экологическому, технологическому и атомному надзору» (вместе с «Положением об организации работы по подготовке и аттестации специалистов организаций, поднадзорных Федеральной службе по экологическому, технологическому и атомному надзору», «Положением об организации обучения и проверки знаний рабочих организаций, поднадзорных Федеральной службе по экологическому, технологическому и атомному надзору»).

Перечень моих персональных данных, на обработку которых я даю согласие:

- фамилия, имя, отчество, дата и место рождения, гражданство;
- прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- владение иностранными языками и языками народов Российской Федерации;
- образование (когда и какие образовательные учреждения закончил(а);
- наименование документа об образовании; номер, серия документа об образовании, направление подготовки или специальность, квалификация по документу об образовании);
- послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
- выполняемая работа с начала трудовой деятельности (включая военную службу); сведения о трудовом стаже;
- должность и место работы;
- государственные награды, иные награды и знаки отличия (кем награжден и когда);
- адрес регистрации по месту жительства и фактического проживания;
- дата регистрации по месту жительства;
- паспорт (серия, номер, кем и когда выдан, номер подразделения);
- данные водительского удостоверения (серия, номер, категория, дата выдачи, срок действия, стаж вождения);
- сведение об имуществе (наличие личного автомобиля) и данных документа (ПТС, свидетельство о регистрации автомобиля);
- номер телефона(домашний, мобильный, корпоративный);
- ИНН;
- номер страхового свидетельства обязательного пенсионного страхования;

- результаты предварительных и повторных обязательных медицинских осмотров (обследований);
- данные медицинского полиса добровольного медицинского страхования (номер, программа страхования, срок действия);
- график работы;
- система оплаты труда;
- должностной оклад (часовая ставка);
- условия налоговых вычетов;
- сведения о доходах;
- реквизиты банковских счета и карты, указанные для выплаты заработной платы и иных денежных средств, причитающихся в процессе трудовой деятельности;
- сведения о планируемом отпуске;
- адрес личной электронной почты (e-mail);

Также я даю согласие Оператору для обработки специальных категорий персональных и иных данных:

- обработку сведений о моем состоянии здоровья по результатам предварительного и периодических медицинских осмотров; категория инвалидности и данные МСЭК (при наличии);

- обработку сведений, которые используются Оператором для установления моей личности и для размещения на сайте компании, доске почета Оператора, информационной доске Оператора, отражающей работу с персоналом (моя фотография, кадры видеосъемки с моим изображением, образцы почерка и подписи);

-получение моих персональных данных о предыдущих местах работы и периодах трудовой деятельности от третьих лиц с целью сбора информации о моем трудовом опыте;

Согласие Оператору предоставляется на осуществление действий в отношении моих персональных данных, как Работника Оператора, которые необходимы для достижения вышеуказанных целей, а также для передачи третьим лицам :[2]

Кому, и с какой целью	**Персональные данные**	**Разрешаю /не разрешаю** (необходимо своей рукой указать – «да» в случае разрешения, либо «нет» в случае запрета передачи информации)
Компании, оказывающей услуги Оператору на основе договора в части обработки персональных данных как в информационных системах Оператора, так и на бумаж-	Фамилия, имя, отчество Дата, месяц, год рождения Пол Паспортные данные Данные водительского удостоверения Гражданство Адрес прописки	

[2] В таблице, при получении согласия, должны быть прописаны конкретные организации

ных носителях для осуществления кадрового администрирования, для отражения и учета взаиморасчетов между Работником и Оператором **ООО «УСЦ ЕвроСиб-Энерго»,** **ООО «Эн+ Диджитал»**	Адрес фактического проживания СНИЛС ИНН Телефонный номер(домашний/мобильный) Семейной положение Сведения о составе семьи и членах семьи Сведения об образовании Сведения о повышении квалификации (период, вид повышения квалификации, наименование образовательного учреждения, наименование документа, подтверждающего повышение квалификации, номер и серия документа) Сведения о профессиональной переподготовке (период, вид профессиональной переподготовки, наименование специальности, наименование документа, подтверждаемого профессиональную переподготовку, номер и серия документа) Сведения о страховом стаже Сведения о наградах, поощрениях Сведения об отпусках, командировках и других причинах отсутствия на работе (дата начала, дата окончания, количество дней, вид отсутствия) Сведения о воинском учете Структурное подразделение Профессия/должность График работы Система оплаты труда Должностной оклад/ставка Сведения о начисленной заработной плате Сведения о доходах с предыдущего места работы Сведения о допуске к работам (вид допуска, дата получения, срок действия) Сведения о прохождении медицинских осмотров (периодичность прохождения, дата последнего медосмотра) Сведения о наличии/отсутствии инвалидности Стаж работы на предприятии Условия налоговых вычетов (личный вычет, вычеты на детей, имущественные, статус налогоплательщика, льготы как подвергшимся воздействию радиации) Зарплатный счет Данные медицинского полиса добровольного медицинского страхования (номер, программа страхования, срок действия)	

	Номер избирательного участка Сведения об отпуске (ежегодном оплачиваемом и дополнительном)	
Банку для оформления: - банковской карты и перечисления на нее заработной платы; - электронной цифровой подписи для подтверждения/продления полномочий **- Банк «СОЮЗ» (АО);** **-ПАО «Сбербанк»;** **-ГПБ (АО);** **-Банк ВТБ (ПАО);** **-ФИЛИАЛ "АТБ" (ПАО) В Г.УЛАН-УДЭ;** **-ИРКУТСКИЙ РФ АО "РОССЕЛЬХОЗБАНК";** **-ООО "ХКФ БАНК";** **-АЗИАТСКО-ТИХООКЕАНСКИЙ БАНК (ПАО).** **-Банк «СОЮЗ» (АО);** **-ПАО «Сбербанк»;** **-ГПБ (АО);** **- ПАО «Райффайзенбанк»;** **- ВБРР (АО);** **- ПАО Банк «ФК Открытие»** **- АО «Россельхозбанк»**	Фамилия, имя, отчество Место работы Должность	
Третьим лицам для оформления электронной цифровой подписи и подтверждения/продления полномочий с целью осуществления закупочной деятельности Оператора **НПФ «Форус», ООО «ТД «ЕвроСибЭнерго»**	Фамилия, имя, отчество Дата, месяц, год рождения Паспортные данные Адрес прописки Адрес фактического проживания СНИЛС	
Страховой компании – для оформления полиса обязательного и добровольного медицинского страхования и третьим лицам (медицинским учреждениям) для оказания медицинских услуг при страховом случае с Работником **- СПАО «Ингосстрах»**	Фамилия, имя, отчество Дата, месяц, год рождения Паспортные данные Адрес прописки Адрес фактического проживания Телефонный номер (домашний, мобильный)	
Компании, оказывающей типографские и издательские	Фамилия, имя, отчество Структурное подразделение	

услуги – для оформления визитных карточек, изготовления табличек на двери, издания корпоративной газеты	Должность Номер мобильного рабочего телефона Номер рабочей электронной почты (e-mail); Фото	
Кредитным организациям, в которые обращался Работник для оформления и выдачи кредитов, получения иных услуг при условии, что Работник заранее сообщил Оператору наименования указанных кредитных организаций при запросе справки (сверяется по журналу обращений Работников)	Фамилия, имя, отчество Структурное подразделение Должность Стаж работы Уровень заработной платы	
Третьим лицам для оформления визы, приглашения на въезд в иностранные государства, приобретение авиа и железнодорожных билетов, заказа гостиниц	Фамилия, имя, отчество Дата, месяц, год рождения Паспортные данные, в том числе заграничного паспорта Гражданство Адрес регистрации и фактического места жительства	
Медицинскому центру, с которым заключен договор на организацию проведения первичного и повторного медицинского осмотра на предмет годности к осуществлению трудовых обязанностей	Фамилия, имя, отчество Дата, месяц, год рождения Структурное подразделение Должность/профессия или вид работ	
Учебным центрам и организациям – для организации обучения, участия в семинарах, конференциях – **ННОУ УЦ КУ «ЕвроСиб-Энерго», другим организациям**	Фамилия, имя, отчество Дата, месяц, год рождения Структурное подразделение Должность/профессия или вид работ Учебные заведения, в которых работник учился и периодов учебы Вид документа об образовании, номер, серия Специальность Квалификация Стаж работы в данной области	
Аудиторской организации с целью соблюдения законодательства при проведении обязательного аудита	Фамилия, имя, отчество Дата, месяц, год рождения Структурное подразделение Должность/профессия или вид работ Взаиморасчеты между Работником и Оператором	

	Иные документы по запросу, связанные с осуществлением трудовой функции Работника, а Оператором - исполнения законодательства	
Министерствам, органам исполнительной власти с целью поощрения, награждения и иным организациям, оказывающим услуги Оператору на основе договора в части оказания консультационных услуг, связанных с подготовкой и получением ведомственных наград **Министерству энергетики Российской Федерации; Министерству жилищной политики, энергетики и транспорта Иркутской области;**	Фамилия, имя, отчество Дата, месяц, год рождения Структурное подразделение Должность/профессия или вид работ Учебные заведения, в которых работник учился и периодов учебы Вид документа об образовании, номер, серия Специальность Квалификация Стаж работы в данной области Записи в трудовой книжке	
Представителям трудового коллектива для публичного обращения при вручении наград, поощрении, поздравлении со знаменательными событиями в жизни (день рождение, бракосочетание, рождение детей), выражения соболезнования при смерти близкого родственника	Фамилия, имя, отчество Число и месяц рождения Структурное подразделение Должность/профессия или вид работ Стаж работы в данной области Стаж работы на предприятии О заслугах в трудовой деятельности	
Государственные и муниципальные службы с целью выполнения ст.64.1 ТК РФ	Фамилия, имя, отчество Число, месяц, год и место рождения Должность государственной или муниципальной службы, замещаемая гражданином непосредственно перед увольнением с государственной или муниципальной службы Наименование организации Дата и номер приказа Дата заключения трудового договора и срок, на который он заключен (указывается дата начала работы, а в случае, если заключается срочный трудовой договор, - срок его действия и обстоятельства (причины), послужившие основанием для заключения срочного трудового договора) Профессия/должность Род деятельности	
Размещение информации на	Фамилия, имя, отчество	

корпоративных интернет-ресурсах, в корпоративном печатном издании **ЗАО «Газета Восточно-Сибирская правда» (Сибирский энергетик»)**	Должность Фото Учебные заведения, в которых работник учился, периодов учебы, ученая степень Дата трудоустройства Стаж работы в данной области Стаж работы на предприятии О заслугах, наградах и поощрениях в трудовой деятельности	
Компании, оказывающей услуги Оператору на основе договора в части проведения специальной оценки условий труда рабочих мест Оператора	Фамилия, имя, отчество Профессия/должность Структурное подразделение СНИЛС	
Компании, оказывающей услуги Оператору на основе договора в части предоставления услуг корпоративной подвижной радиотелефонной связи (мобильной, сотовой) (ООО «Т2 Мобайл», ПАО «МТС», ПАО «МегаФон», ПАО «Ростелеком», ПАО «ВымпелКом»)	Фамилия, имя, отчество Дата, месяц, год рождения Пол Паспортные данные Адрес прописки Адрес фактического проживания	

В случае изменения моих персональных данных в течение срока трудового договора обязуюсь проинформировать об этом Оператора.

Обработка вышеуказанных персональных данных будет осуществляться автоматизировано, а также без использования средств автоматизации; с передачей по внутренней сети юридического лица; с передачей по сети Интернет, электронных переносных носителях.

Настоящее согласие может быть мною отозвано, путем направления письменного уведомления.
Я уведомлен, что при отзыве мной согласия на обработку персональных данных Оператор вправе продолжить обработку моих персональных в случаях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Требование об уничтожении не распространяется на персональные данные, для которых нормативными правовыми актами предусмотрена обязанность их хранения, в том числе после прекращения трудовых отношений.

С Политикой Общества в отношении обработки персональных данных я ознакомлен.

Дата начала обработки персональных данных: _____ (число, месяц, год)

Настоящее согласие действует в течение всего срока рассмотрения моей кандидатуры,

а в случае заключения трудового договора - на срок действия трудового договора.

(подпись Субъекта)	(Ф.И.О. Субъекта)

Приложение № 2

Журнал учета нештатных ситуаций (типовая форма)

№	ДДата	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 № 3

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

1. Информационные системы.

Информационная система является информационной системой, обрабатывающей специальные категории персональных данных (ИСПДн-С), если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные (ИСПДн-Б), если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные (ИСПДн-О), если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей иные категории персональных данных (ИСПДн-И), если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

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

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

3. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18 [1] Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

4. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

5. Необходимость обеспечения 1-го уровня защищенности персональных данных (УЗ-1) при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

6. Необходимость обеспечения 2-го уровня защищенности персональных данных (УЗ-2) при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7. Необходимость обеспечения 3-го уровня защищенности персональных данных (УЗ-3) при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система

обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

8. Необходимость обеспечения 4-го уровня защищенности персональных данных (УЗ-4) при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

9. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

10. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 9, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

11. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 10, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

12. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в

информационных системах помимо требований, предусмотренных пунктом 11, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Тип ИСПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн-С	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да				
ИСПДн-Б			УЗ-1	УЗ-2	УЗ-3
ИСПДн-И	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				
ИСПДн-О	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4

Приложение № 4

Акт классификации ИСПДн
по уровню защищенности (примерная форма).

УТВЕРЖДАЮ
Председатель комитета по управлению
информационной безопасностью
« ____ » _____ 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: только сотрудники оператора/не являющихся сотрудниками оператора. Тип ИСПДн: ИСПДн-С / ИСПДн-Б / ИСПДн-И / ИСПДн-О.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

2. Объем обрабатываемых персональных данных: менее 100 000/ более 100 000.

Одновременно обрабатываются данные менее чем 100 000 субъектов персональных данных.
Одновременно обрабатываются данные более 100 000 субъектов персональных данных.

3. Требуемые характеристики безопасности персональных данных: целостность, доступность, конфиденциальность, защищенность от уничтожения, изменения, блокирования и проч.

Необходимо выполнить следующие характеристики безопасности персональных данных: целостность, доступность, конфиденциальность, защищенность от уничтожения, изменения, блокирования и проч.

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 анализа исходных данных информационной системы и в соответствии с Постановлением Правительства Российский Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

РЕШИЛА

Установить информационной системе «Наименование ИСПДн» Уровень Защищенности УЗ-1/2/3/3.

«_____»_____201_ г.

Председатель комиссии _____ _____

Члены комиссии

_____ _____

_____ _____

_____ _____

Приложение № 5

Частная модель угроз ИСПДн (примерная форма).

УТВЕРЖДАЮ
Председатель комитета по управлению
информационной безопасностью

« ____ » _____ 201_ г.

Частная модель угроз

безопасности персональных данных

в информационной системе персональных данных

«Наименование ИСПДн»

201_ г. Иркутск.

Оглавление

1. Исходные данные об ИСПДн.

1.1. Владелец ИСПДн.

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

1.2. Цель обработки персональных данных

<Регистрация сведений, необходимых для осуществления ООО «УСЦ ЕвроСибЭнерго» уставной деятельности>

1.3. 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.

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

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

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

1.5.1. 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.

1.5.2. Границы контролируемых зон.

Контролируемыми зонами являются здания в которых располагаются структурные единицы.

1.6. Топология ИСПДн и конфигурация ее отдельных компонентов.

1.6.1. Топология ИСПДн.

Основными составляющими ИСПДн являются:

- центральный узел обработки данных;
- узел администрирования;
- автоматизированные рабочие места (АРМ) сотрудников.

1.7. Конфигурация отдельных компонентов ИСПДн.

1.7.1. 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.

1.7.2. Узел администрирования.

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

1.7.3. 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.

1.8. Связи между основными компонентами ИСПДн.

1.8.1. 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.

1.8.2. 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;

1.8.3. 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).

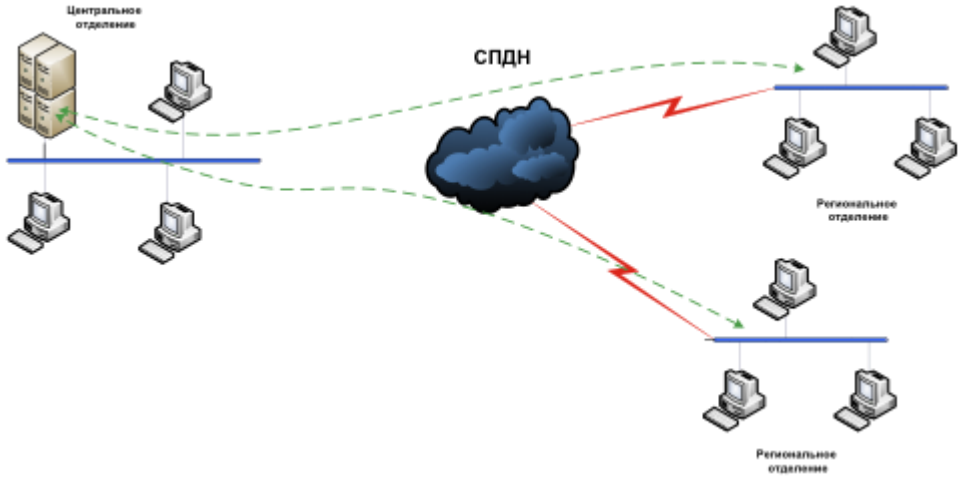

Рисунок 1. Схема ИСПДн и информационных потоков в ней.

1.9. 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.

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

В обработке персональных данных участвует следующее общесистемное программное обеспечение:

- ОС Unix;
- ОС Windows 2003/2008/2012/XP/Vista/Windows7.

В обработке персональных данных участвует следующее прикладное программное обеспечение:

- ПО «Автоматизированная система v.1»;
- СУБД Oracle.

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

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

1.11.1. 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.

1.11.2. 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.

2. 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).

2.1. 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.

2.2. 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									
	К0	К1	К2	К3	К4	К5	К6	К7	К8	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	2	2	0	0	5	2	5	5	5	5

вредоносных программ										
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 несанкционирован-	5	5	0	0	0	0	0	0	0	5

ного изменения маршрутно-адресных данных										
угрозы внедрения по сети вредоносных программ	2	2	0	0	2	2	2	2	0	2

2.3. 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

2.4. 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

2.5. 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 6.

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 уровня защищенности ИСПДн УЗ-1/2/3/4 .

«_____»_____201 _ г.

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

Лист регистрации изменений

№ пп	Основание[3]	Срок введения изменения	Изменения внёс			Примечания
			ФИО	Подпись	Дата внесения изменения	
1.	Приказ от 06.11.2018 №06.001-01-2.1-0583	06.11.2018	Бояркина Е.Ю.		06.11.2018	Изм. Прил.1

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

ИРКУТСКАЯ
ЭЛЕКТРОСЕТЕВАЯ КОМПАНИЯ

Открытое акционерное общество «Иркутская электросетевая компания» (ОАО «ИЭСК»)

ПРИКАЗ

21.03.2017 № 06.001-01-2.1-0099/1

О введении в действие
стандартов предприятия по
информационной безопасности

В соответствии с планом стандартизации ОАО «ИЭСК», а также в связи с переводом части функций из состава обеспечивающего процесса ОАО «ИЭСК» «Управление информационными технологиями» на аутсорсинг.

ПРИКАЗЫВАЮ:

1. Ввести в действие с даты регистрации настоящего приказа:
   1.1. СТП 001.017.062-2016 «Политика в области информационной безопасности ОАО «ИЭСК»,
   1.2. СТП 001.017.063-2016 «Система управления информационной безопасностью ОАО «ИЭСК»,
   1.3. СТП 001.017.064-2016 «Управление доступом к информационным ресурсам ИС ОАО «ИЭСК»,
   1.4. СТП 001.017.065-2016 «Управление паролями»,
   1.5. СТП 001.017.066-2016 «Аудит информационной безопасности»,
   1.6. СТП 001.017.067-2016 «О защите персональных данных»,
   1.7. СТП 001.017.068-2016 «Обеспечение информационной безопасности платежных систем»,
   1.8. СТП 001.017.069-2016 «Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации»,
   1.9. СТП 001.017.070-2016 «Процедура планирования и реализации контрмер информационной безопасности»;
2. С даты регистрации настоящего приказа отменить действие СТП 001.004.031-2014 «Политика в области информационной безопасности», СТП 001.004.010-2016 «Управление доступом к информационным ресурсам», СТП 001.004.008-2013 «О защите персональных данных»;
3. Директорам филиалов, Директорам по функциональным направлениям, руководителям структурных подразделений исполнительной дирекции обеспечить ознакомление подчиненного персонала с требованиями СТП в течение 10 рабочих дней с даты получения настоящего приказа;
4. Руководителям дочерних зависимых обществ (ДЗО) ОАО «ИЭСК» рекомендовать СТП к адаптации и применению в ДЗО.
5. Начальнику САСТУ Скольжикову Е.В.
   5.1. в течение 10 рабочих дней с даты получения настоящего приказа письменно уведомить ООО «УСЦ Евросибэнерго» о вводе в действие СТП в целях надлежащего исполнения обязательств по договору услуг №016-ИТ 01 от 11.11.2015.
   5.2. в течении 30 рабочих дней с даты регистрации настоящего приказа внести изменения в действующий регламент взаимодействия между Исполнителем и Заказчиком в рамках договора оказания услуг №016-ИТ 01 от 11.11.2015.
6. Начальнику ОУБПС Русанову Р.В. организовать размещение стандартов на обменном диске \\iesk-s-fs0101\ENTERPRIZE\01_STANDART, а также обеспечить регистрацию и хранение актуальной версии стандарта в системе электронного документооборота.

664033, г.Иркутск, ул. Лермонтова 257, Тел.: (3952) 792-459 Факс: (3952) 792-461E-mail: iesk@irkutskenergo.ru
ОКПО 77642878 ОГРН 1093850013762 ИНН/КПП 3812122706/997450001

7. Контроль исполнения СТП и данного приказа возложить на директора по безопасности и режиму Облова А.А.

Директор по передаче электроэнергии –
главный инженер
(приказ от 16.03.2017 №54-ЛС и
доверенность № юр-205 от 29.06.2016) Ю.Н. Терских

ИРКУТСКАЯ
ЭЛЕКТРОСЕТЕВАЯ КОМПАНИЯ

Открытое акционерное общество «Иркутская электросетевая компания» (ОАО «ИЭСК»)

ПРИКАЗ

06.11.2018 № 06.001-01-2.1-0583

О сборе согласий на обработку персональных данных и внесении изменений в СТП 001.017.067-2016 «О защите персональных данных»

В целях исполнения требований Федерального закона "О персональных данных" от 27.07.2006 № 152-ФЗ, в соответствии с СТП 001.017.067-2016 «О защите персональных данных», в связи с расширением круга третьих лиц – контрагентов ОАО «ИЭСК»

ПРИКАЗЫВАЮ:

1. Организовать заполнение и сбор письменных согласий на передачу и обработку персональных данных работников филиалов и Исполнительной дирекции по форме приложения к настоящему приказу. Срок – 23.11.2018. Ответственные: по филиалам – директора филиалов, по Исполнительной дирекции – директор по персоналу.

2. Процедуру заполнения и сбора письменных согласий организовать в соответствии с Регламентом взаимодействия сторон при исполнении договора возмездного оказания услуг по кадровому делопроизводству между ОАО «ИЭСК» и ООО «УСЦ «ЕвроСибЭнерго» (введен в действие приказом № 06.001-01-2.1-0272 от 18.07.2017).

3. Директорам филиалов обеспечить неограниченный доступ к СТП 001.004.005-2014 «Политика в отношении обработки персональных данных» для работников филиалов.

4. Начальнику ОУБПС Русанову Р.В. - внести изменения в оригинал СТП 001.017.067-2016 «О защите персональных данных» – изложить приложение 1 к СТП в редакции приложения к настоящему приказу; разместить актуальную версию СТП на сетевом ресурсе I:\01_STANDART, а также в системе электронного документооборота. Срок – 12.11.2018.

5. Директорам по функциональным направлениям, директорам филиалов, руководителям структурных подразделений ИД - организовать ознакомление подчиненного персонала с изменениями стандарта и обеспечить его исполнение.

6. Контроль исполнения настоящего приказа возложить на филиалах – на директора филиала, в Исполнительной дирекции – на директора по персоналу Сорока А.В.

Директор по передаче электроэнергии –
главный инженер
(приказ от 03.07.2018 № 164-ЛС и Устав) Ю.Н. Терских

664033, г.Иркутск, ул. Лермонтова 257, Тел.: (3952) 792-459, Факс: 792-461,E-mail: iesk@irkutskenergo.ru
ОКПО 77642878 ОГРН 1093850013762 ИНН/КПП 3812122706/381250001

Приложение
к приказу от 06.11.2018
№ 06.001-01-2.1-0583

Исполняющему обязанности Генерального директора
ОАО «ИЭСК» Терских Ю.Н.

от

_____
(Ф.И.О.)

Согласие на передачу и обработку персональных данных

Я, ***ФИО, паспорт (серия, номер, выдан), зарегистрированный по адресу (адрес регистрации)***, в соответствии с нормативными правовыми актами Российской Федерации, регулирующими вопросы защиты персональных данных работников, свободно, своей волей и в своем интересе даю согласие ***Открытому акционерному обществу «Иркутская электросетевая компания» (ОАО «ИЭСК»),*** далее – Оператор, адрес ***г. Иркутск, ул. Лермонтова, 257***: на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 статьи 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных",
в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения, исполнения, оформления и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления и выплаты заработной платы и иных платежей с использованием банковской карты;
- исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ;
- предоставления сведений в банк для оформления банковской карты и перечисления на нее заработной платы;
- предоставления сведений третьим лицам для оформления полиса ДМС;
- предоставления налоговых вычетов;
- обучения, повышения квалификации, переобучения, продвижения по службе;
- контроля количества и качества выполняемой мной работы;
- обеспечения сохранности моего имущества и Оператора;
- предоставления гарантий и льгот, предусмотренных нормативными правовыми актами, локальными нормативными актами, соглашениями, трудовым договором;
- включения в корпоративные справочники и другие общественно доступные источники информации Оператора (в том числе размещение информации на корпоративных интернет-ресурсах (сайтах));
- идентификации и аутентификации меня в информационных системах,
- публичное обращение, публичное поздравление с днем рождения, юбилеями;
- страхования жизни и здоровья;

- проведения статистических и иных исследований и опросов;
- создания и ведения информационных систем - "1С: Зарплата и управление персоналом".
- оформления и приобретения авиа- и железнодорожных билетов;
- оформления доверенностей на представление интересов ОАО «ИЭСК»;
- участия в корпоративных проектах развития персонала;
- проведения аттестации;
- формирования Плана преемственности и кадрового резерва;
- контроля прохождения через систему доступа (при наличии автоматизированной программы учета доступа) в здание, к месту работы;
- для ведения реестра аттестационных комиссий предприятий (Личные данные членов комиссий по проверке знаний норм и правил работы в электроустановках (Ф.И.О., сведения об образовании, № диплома и дата выдачи, дата последнего повышения квалификации по должности;
- для прохождения аттестации в Ростехнадзоре (согласно Приказа Ростехнадзора от 29.01.2007 N 37 (ред. от 27.08.2010) «О порядке подготовки и аттестации работников организаций, поднадзорных Федеральной службе по экологическому, технологическому и атомному надзору» (вместе с «Положением об организации работы по подготовке и аттестации специалистов организаций, поднадзорных Федеральной службе по экологическому, технологическому и атомному надзору», «Положением об организации обучения и проверки знаний рабочих организаций, поднадзорных Федеральной службе по экологическому, технологическому и атомному надзору»).

Перечень моих персональных данных, на обработку которых я даю согласие:

- фамилия, имя, отчество, дата и место рождения, гражданство;
- прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- владение иностранными языками и языками народов Российской Федерации;
- образование (когда и какие образовательные учреждения закончил(а);
- наименование документа об образовании; номер, серия документа об образовании, направление подготовки или специальность, квалификация по документу об образовании);
- послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
- выполняемая работа с начала трудовой деятельности (включая военную службу); сведения о трудовом стаже;
- должность и место работы;
- государственные награды, иные награды и знаки отличия (кем награжден и когда);
- адрес регистрации по месту жительства и фактического проживания;
- дата регистрации по месту жительства;
- паспорт (серия, номер, кем и когда выдан, номер подразделения);
- данные водительского удостоверения (серия, номер, категория, дата выдачи, срок действия, стаж вождения);
- сведение об имуществе (наличие личного автомобиля) и данных документа (ПТС, свидетельство о регистрации автомобиля);
- номер телефона(домашний, мобильный, корпоративный);
- ИНН;
- номер страхового свидетельства обязательного пенсионного страхования;
- результаты предварительных и повторных обязательных медицинских осмотров (обследований);

- данные медицинского полиса добровольного медицинского страхования (номер, программа страхования, срок действия);
- график работы;
- система оплаты труда;
- должностной оклад (часовая ставка);
- условия налоговых вычетов;
- сведения о доходах;
- реквизиты банковских счета и карты, указанные для выплаты заработной платы и иных денежных средств, причитающихся в процессе трудовой деятельности;
- сведения о планируемом отпуске;
- адрес личной электронной почты (e-mail);

Также я даю согласие Оператору для обработки специальных категорий персональных и иных данных:
- обработку сведений о моем состоянии здоровья по результатам предварительного и периодических медицинских осмотров; категория инвалидности и данные МСЭК (при наличии);
- обработку сведений, которые используются Оператором для установления моей личности и для размещения на сайте компании, доске почета Оператора, информационной доске Оператора, отражающей работу с персоналом (моя фотография, кадры видеосъемки с моим изображением, образцы почерка и подписи);
-получение моих персональных данных о предыдущих местах работы и периодах трудовой деятельности от третьих лиц с целью сбора информации о моем трудовом опыте;

Согласие Оператору предоставляется на осуществление действий в отношении моих персональных данных, как Работника Оператора, которые необходимы для достижения вышеуказанных целей, а также для передачи третьим лицам :

Кому, и с какой целью	**Персональные данные**	**Разрешаю /не разрешаю** (необходимо своей рукой указать – «да» в случае разрешения, либо «нет» в случае запрета передачи информации)
Компании, оказывающей услуги Оператору на основе договора в части обработки персональных данных как в информационных системах Оператора, так и на бумажных носителях для осуществления кадрового администрирования, для отражения и учета взаиморасчетов между Работником и Оператором	Фамилия, имя, отчество Дата, месяц, год рождения Пол Паспортные данные Данные водительского удостоверения Гражданство Адрес прописки Адрес фактического проживания СНИЛС ИНН Телефонный номер(домашний/мобильный) Семейной положение Сведения о составе семьи и членах семьи	

- ООО «УСЦ ЕвроСибЭнерго»; **- ООО «Эн+ Диджитал»;**	Сведения об образовании Сведения о повышении квалификации (период, вид повышения квалификации, наименование образовательного учреждения, наименование документа, подтверждающего повышение квалификации, номер и серия документа) Сведения о профессиональной переподготовке (период, вид профессиональной переподготовки, наименование специальности, наименование документа, подтверждаемого профессиональную переподготовку, номер и серия документа) Сведения о страховом стаже Сведения о наградах, поощрениях Сведения об отпусках, командировках и других причинах отсутствия на работе (дата начала, дата окончания, количество дней, вид отсутствия) Сведения о воинском учете Структурное подразделение Профессия/должность График работы Система оплаты труда Должностной оклад/ставка Сведения о начисленной заработной плате Сведения о доходах с предыдущего места работы Сведения о допуске к работам (вид допуска, дата получения, срок действия) Сведения о прохождении медицинских осмотров (периодичность прохождения, дата последнего медосмотра) Сведения о наличии/отсутствии инвалидности Стаж работы на предприятии Условия налоговых вычетов (личный вычет, вычеты на детей, имущественные, статус налогоплательщика, льготы как подвергшимся воздействию радиации) Зарплатный счет Данные медицинского полиса добровольного медицинского страхования (номер, программа страхования, срок действия) Номер избирательного участка Сведения об отпуске (ежегодном оплачиваемом и дополнительном)	
Банку для оформления: - банковской карты и перечисления на нее	Фамилия, имя, отчество Место работы Должность	

заработной платы; - электронной цифровой подписи для подтверждения/продления полномочий **- Банк «СОЮЗ» (АО);** **- ПАО «Сбербанк»;** **- ГПБ (АО);** **- Банк ВТБ (ПАО);** **- ФИЛИАЛ "АТБ" (ПАО) В Г.УЛАН-УДЭ;** **- ИРКУТСКИЙ РФ АО "РОССЕЛЬХОЗБАНК";** **- ООО "ХКФ БАНК";** **- АЗИАТСКО-ТИХООКЕАНСКИЙ БАНК (ПАО);** **- ПАО «Райффайзенбанк»;** **- ВБРР (АО);** **- ПАО Банк «ФК Открытие»** **- АО «Россельхозбанк»;**		
Третьим лицам для оформления электронной цифровой подписи и подтверждения/продления полномочий с целью осуществления закупочной деятельности Оператора **- НПФ «Форус»;** **- ООО «ТД «ЕвроСибЭнерго»;**	Фамилия, имя, отчество Дата, месяц, год рождения Паспортные данные Адрес прописки Адрес фактического проживания СНИЛС	
Страховой компании – для оформления полиса обязательного и добровольного медицинского страхования и третьим лицам (медицинским учреждениям) для оказания медицинских услуг при страховом случае с Работником **- СПАО «Ингосстрах»;**	Фамилия, имя, отчество Дата, месяц, год рождения Паспортные данные Адрес прописки Адрес фактического проживания Телефонный номер (домашний, мобильный)	
Компании, оказывающей типографские и издательские услуги – для оформления визитных карточек, изготовления табличек на двери, издания корпоративной газеты	Фамилия, имя, отчество Структурное подразделение Должность Номер мобильного рабочего телефона Номер рабочей электронной почты (e-mail); Фото	

Кредитным организациям, в которые обращался Работник для оформления и выдачи кредитов, получения иных услуг при условии, что Работник заранее сообщил Оператору наименования указанных кредитных организаций при запросе справки (сверяется по журналу обращений Работников)	Фамилия, имя, отчество Структурное подразделение Должность Стаж работы Уровень заработной платы	
Третьим лицам для оформления визы, приглашения на въезд в иностранные государства, приобретение авиа и железнодорожных билетов, заказа гостиниц	Фамилия, имя, отчество Дата, месяц, год рождения Паспортные данные, в том числе заграничного паспорта Гражданство Адрес регистрации и фактического места жительства	
Медицинскому центру, с которым заключен договор на организацию проведения первичного и повторного медицинского осмотра на предмет годности к осуществлению трудовых обязанностей	Фамилия, имя, отчество Дата, месяц, год рождения Структурное подразделение Должность/профессия или вид работ	
Учебным центрам и организациям – для организации обучения, участия в семинарах, конференциях – **- ННОУ УЦ КУ «ЕвроСибЭнерго»;** **- другим организациям;**	Фамилия, имя, отчество Дата, месяц, год рождения Структурное подразделение Должность/профессия или вид работ Учебные заведения, в которых работник учился и периодов учебы Вид документа об образовании, номер, серия Специальность Квалификация Стаж работы в данной области	
Аудиторской организации с целью соблюдения законодательства при проведении обязательного аудита	Фамилия, имя, отчество Дата, месяц, год рождения Структурное подразделение Должность/профессия или вид работ Взаиморасчеты между Работником и Оператором Иные документы по запросу, связанные с осуществлением трудовой функции Работника, а Оператором - исполнения законодательства	
Министерствам, органам исполнительной власти с целью поощрения,	Фамилия, имя, отчество Дата, месяц, год рождения Структурное подразделение	

награждения и иным организациям, оказывающим услуги Оператору на основе договора в части оказания консультационных услуг, связанных с подготовкой и получением ведомственных наград **- Министерству энергетики Российской Федерации;** **- Министерству жилищной политики, энергетики и транспорта Иркутской области;**	Должность/профессия или вид работ Учебные заведения, в которых работник учился и периодов учебы Вид документа об образовании, номер, серия Специальность Квалификация Стаж работы в данной области Записи в трудовой книжке	
Представителям трудового коллектива для публичного обращения при вручении наград, поощрении, поздравлении со знаменательными событиями в жизни (день рождение, бракосочетание, рождение детей), выражения соболезнования при смерти близкого родственника	Фамилия, имя, отчество Число и месяц рождения Структурное подразделение Должность/профессия или вид работ Стаж работы в данной области Стаж работы на предприятии О заслугах в трудовой деятельности	
Государственные и муниципальные службы с целью выполнения ст.64.1 ТК РФ	Фамилия, имя, отчество Число, месяц, год и место рождения Должность государственной или муниципальной службы, замещаемая гражданином непосредственно перед увольнением с государственной или муниципальной службы Наименование организации Дата и номер приказа Дата заключения трудового договора и срок, на который он заключен (указывается дата начала работы, а в случае, если заключается срочный трудовой договор, - срок его действия и обстоятельства (причины), послужившие основанием для заключения срочного трудового договора) Профессия/должность Род деятельности	
Размещение информации на корпоративных интернет-ресурсах, в корпоративном печатном издании	Фамилия, имя, отчество Должность Фото Учебные заведения, в которых работник	

- ЗАО «Газета Восточно-Сибирская правда» (Сибирский энергетик»)	учился, периодов учебы, ученая степень Дата трудоустройства Стаж работы в данной области Стаж работы на предприятии О заслугах, наградах и поощрениях в трудовой деятельности	
Компании, оказывающей услуги Оператору на основе договора в части проведения специальной оценки условий труда рабочих мест Оператора	Фамилия, имя, отчество Профессия/должность Структурное подразделение СНИЛС	
Компании, оказывающей услуги Оператору на основе договора в части предоставления услуг корпоративной подвижной радиотелефонной связи (мобильной, сотовой) **- ООО «Т2 Мобайл»** **- ПАО «МТС»** **- ПАО «МегаФон»** **- ПАО «Ростелеком»** **- ПАО «ВымпелКом»**	Фамилия, имя, отчество Дата, месяц, год рождения Пол Паспортные данные Адрес прописки Адрес фактического проживания	

В случае изменения моих персональных данных в течение срока трудового договора обязуюсь проинформировать об этом Оператора.

Обработка вышеуказанных персональных данных будет осуществляться автоматизировано, а также без использования средств автоматизации; с передачей по внутренней сети юридического лица; с передачей по сети Интернет, электронных переносных носителях.

Настоящее согласие может быть мною отозвано, путем направления письменного уведомления.
Я уведомлен, что при отзыве мной согласия на обработку персональных данных Оператор вправе продолжить обработку моих персональных в случаях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Требование об уничтожении не распространяется на персональные данные, для которых нормативными правовыми актами предусмотрена обязанность их хранения, в том числе после прекращения трудовых отношений.

С Политикой Общества в отношении обработки персональных данных я ознакомлен.

Дата начала обработки персональных данных: _____ (число, месяц, год)

Настоящее согласие действует в течение всего срока рассмотрения моей кандидатуры, а в случае заключения трудового договора - на срок действия трудового договора.

_____ _____

(подпись Субъекта) (Ф.И.О. Субъекта)