УТВЕРЖДЕНО

Генеральный директор
АО «ЭнСер»
_____М.А. Ефимов
«_21_» _сентября_ 2023г.

ПОЛОЖЕНИЕ

Об обработке и защите персональных данных работников АО «ЭнСер»

Содержание

Введение

Настоящее Положение «Об обработке и защите персональных данных работников АО «ЭнСер» (далее по тексту Положение) разработано для описания принципов, правил и иных вопросов обработки персональных данных в Обществе в соответствии с нормами действующего законодательства Российской Федерации, в том числе Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных», Федеральным законом «Об информации, информационных технологиях и о защите информации»», Федеральным законом «О противодействии коррупции».

1. Область применения

1.1. Настоящее Положение устанавливает общие требования к обеспечению безопасности персональных данных, обрабатываемых 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. Настоящее Положение распространяется на все подразделения Общества. Работники Общества, осуществляющие обработку персональных данных, должны быть ознакомлены с настоящим положением.

1.3. Настоящее Положение входит в состав нормативных документов системы управления Общества.

2. Нормативные ссылки

В настоящем положении использованы ссылки на следующие документы:

- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);
- Трудовой кодекс Российской Федерации (далее также – ТК РФ);
- Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Методический документ. Методика оценки угроз безопасности информации, утвержден ФСТЭК России 05 февраля 2021 г.;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена ФСТЭК России 15 февраля 2008 г.;
- 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 «Политика в области информационной безопасности»;
- СТП «Система управления информационной безопасностью»;
- СТП «Управление доступом к информационным ресурсам ИС»;
- СТП «Аудит информационной безопасности»;
- положение или иной внутренний документ Общества (при наличии) по вопросам обработки персональных данных физических лиц для целей их регистрации и (или)

авторизации на сайтах Общества в сети «Интернет», регистрации в качестве участника проводимых Обществом мероприятий, информирования о таких мероприятиях, публикации фотографий и видеозаписей с мероприятий.

3. Определения и сокращения

В настоящем положении используются следующие сокращения и 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.

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

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.

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.

ИТ служба - подразделение (работник) Общества, осуществляющее функции ИТ обеспечения Общества, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.

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.

Общество – Акционерное общество «ЭнСер» (АО «ЭнСер»)

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

Общедоступные персональные данные - персональные данные, сделанные общедоступными субъектом персональных данных либо по его просьбе, в том числе размещенные с его письменного согласия в общедоступных источниках 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).

Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О 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.

Подразделение ИБ - подразделение (работник), ответственное за контроль обеспечения ИБ Общества, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.

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

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

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

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

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

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

Родственники работника - близкие родственники работника, а именно: родители, дети, дедушки, бабушки, внуки, полнородные и неполнородными (имеющие общих отца или мать) братья или сестры.

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 - физическое лицо, обратившееся в Общество с целью поиска работы, либо информация о котором получена из общедоступных источников.

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

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.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства,

иностранному физическому лицу или иностранному юридическому лицу.

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

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

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

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

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

АРМ – автоматизированное рабочее место;
АС – автоматизированная система;
АВС – антивирусные средства;
ВП – выделенное помещение;
ВТСС – вспомогательные технические средства и системы;
ИБ – информационная безопасность;
ИТ – информационные технологии;
ИСПДн – информационная система персональных данных;
КЗ – контролируемая зона;
МЭ – межсетевой экран;
МСЭК - учреждение медико-социальной экспертизы;
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;
СТП - стандарт предприятия;
СВТ – средства вычислительной техники;
СЗИ – средства защиты информации;
СЗПДн – система (подсистема) защиты персональных данных:
СУБД – система управления базами данных;
УБПДн – угрозы безопасности персональным данным;
ФСТЭК – Федеральная служба по техническому и экспортному контролю.

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;

4.1.6. иных принципов, установленных законодательством о 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, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

4.2.3. Общество производит уведомление уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных согласно статье 22 Федерального закона «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:

(1) работники Общества;

(2) бывшие работники Общества;

(3) родственники работников и бывших работников Общества;

(4) соискатели;

(5) физические лица, состоящие или состоявшие в гражданско-правовых и иных отношениях с Обществом (в том числе собственники и пользователи помещений в многоквартирных и жилых домах);

(6) 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;

(7) физические лица - пользователи сайтов Общества в сети «Интернет» (с учетом того, что у Общества может быть в наличии отдельный внутренний документ по вопросам обработки персональных данных физических лиц для данных целей);

(8) представители или работники клиентов и контрагентов Общества - юридических лиц;

(9) посетители офисов Общества.

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, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и другими федеральными законами.

5.2.3. 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:

(1) обработка персональных данных работников Общества может осуществляться с целью организации учета работников Общества, обучения, страхования, продвижения по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы, обеспечения сохранности имущества, проверки конфликта интересов работника, предоставления различного вида льгот и применения иных норм в соответствии с законодательством Российской Федерации и внутренними документами Общества;

(2) обработка персональных данных бывших работников Общества может осуществляться с целью содействия в трудоустройстве, обеспечения личной безопасности, предоставления различного вида льгот и применения иных норм в соответствии с законодательством Российской Федерации и внутренними документами Общества;

(3) обработка персональных данных родственников работников и бывших работников Общества может осуществляться с целью проверки конфликта интересов работника, предоставления различного вида льгот и применения иных норм в соответствии с законодательством Российской Федерации и внутренними документами Общества;

(4) обработка персональных данных соискателей осуществляется с целью содействия в трудоустройстве и заключения трудового договора с Обществом, с возможностью хранения персональных данных в течение определенного срока с момента трудоустройства, указанного в согласии на обработку персональных данных;

(5) обработка персональных данных физических лиц, состоявших или состоящих в гражданско-правовых и иных отношениях с Обществом (в том числе собственников и пользователей помещений в многоквартирных и жилых домах), осуществляется с целью исполнения соответствующих договоров и осуществления Обществом своей хозяйственной деятельности;

(6) обработка персональных данных физических лиц, состоящих или состоявших в договорных и иных отношениях с организациями, которые поручили Обществу в соответствии с договором обрабатывать персональные данные этих физических лиц, может осуществляться с целью исполнения Обществом своих обязательств, установленных таким договором;

(7) обработка персональных данных физических лиц - пользователей сайтов Общества в сети «Интернет» осуществляется с целью использования физическими лицами функциональных возможностей таких сайтов в соответствии с их назначением;

(8) обработка персональных данных представителей или работников клиентов и контрагентов Общества - юридических лиц осуществляется с целью взаимодействия Общества с такими клиентами и контрагентами;

(9) обработка персональных данных физических лиц - посетителей офиса Общества осуществляется с целью взаимодействия с ними.

5.4. Объем и содержание персональных данных

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

(1) объем и содержание персональных данных работников Общества: фамилия, имя, отчество (в том числе предыдущие фамилии, имена и отчества в случае их изменения), дата и место рождения, пол, гражданство, паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, когда и кем выдан), сведения, характеризующие физиологические особенности (изображение лица), адрес места жительства, адрес фактического проживания, контактная информация, сведения об образовании, специальности, квалификации и о наличии специальных знаний и специальной подготовки, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании), сведения о трудовой деятельности, сведения о трудовом и общем стаже, заработной плате и источниках иных доходов (если применимо), 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, сведения о социальных льготах, идентификационный номер налогоплательщика, а также иная информация, необходимая для достижения вышеуказанных целей, и в соответствии с законодательством Российской Федерации;

(2) объем и содержание персональных данных бывших работников Общества: фамилия, имя, отчество (в том числе предыдущие фамилии, имена и отчества в случае их изменения), дата и место рождения, пол, гражданство, паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, когда и кем выдан), сведения, характеризующие физиологические особенности (изображение лица), адрес места жительства, адрес фактического проживания, контактная информация, сведения об образовании, специальности, квалификации и о наличии специальных знаний и специальной подготовки, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании), сведения о трудовой деятельности, сведения о трудовом и общем стаже, сведения о социальных льготах, идентификационный номер налогоплательщика, а также иная информация, необходимая для достижения вышеуказанных целей, и в соответствии с законодательством Российской Федерации;

(3) объем и содержание персональных данных родственников работников и бывших работников Общества: степень родства, фамилия, имя, отчество (в том числе предыдущие фамилии, имена и отчества в случае их изменения), дата и место рождения, сведения об источниках доходов (если применимо), а также иная информация, необходимая для достижения вышеуказанных целей, и в соответствии с законодательством Российской Федерации;

(4) объем и содержание персональных данных соискателей: фамилия, имя, отчество (в том числе предыдущие фамилии, имена и отчества в случае их изменения), 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, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании), сведения о трудовой деятельности, сведения о трудовом и общем стаже, заработной плате и источниках иных доходов (если применимо), 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 в соответствии с законодательством Российской Федерации;

(5) объем и содержание персональных данных физических лиц, состоявших или состоящих в гражданско-правовых и иных отношениях с Обществом (в том числе собственников и пользователей помещений в многоквартирных и жилых домах): фамилия, имя, отчество (в том числе предыдущие фамилии, имена и отчества в случае их изменения), дата и место рождения, пол, гражданство, паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, когда и кем выдан), адрес места жительства, контактная информация, сведения о платежах за потребленные энергоресурсы, идентификационный номер налогоплательщика, а также иная информация, необходимая для достижения вышеуказанных целей, и в соответствии с законодательством Российской Федерации;

(6) 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 персональных данных этих физических лиц, определяется по согласованию сторон такого договора и в соответствии с законодательством Российской Федерации;

(7) объем и содержание персональных данных физических лиц - посетителей сайтов Общества в сети «Интернет»: фамилия, имя, отчество, дата и место рождения, адрес места жительства, контактная информация, данные аккаунтов социальных сетей, сведения об используемом браузере, местоположение и IP-адрес, данные файлов cookie, запрашиваемые интернет-страницы, фотографии и видеозаписи, иная информация, обработка которой определена документами, регулирующими работу сайтов в сети «Интернет», принадлежащих Обществу, и в соответствии с законодательством Российской Федерации;

(8) объем и содержание персональных данных представителей или работников клиентов и контрагентов Общества - юридических лиц: фамилия, имя, отчество, пол, гражданство, паспортные данные или данные иного документа, удостоверяющего личность, адрес места жительства, контактная информация, а также иная информация, необходимая для достижения вышеуказанных целей, и в соответствии с законодательством Российской Федерации;

(9) объем и содержание персональных данных физических лиц - посетителей офиса Общества: фамилия, имя, отчество, паспортные данные или данные иного документа, удостоверяющего личность, контактная информация, а также иная информация, необходимая для достижения вышеуказанных целей, и в соответствии с законодательством Российской Федерации.

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;
- документ об образовании, о квалификации или наличии специальных знаний;
- документы воинского учета.

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

5.6. Сроки обработки персональных данных

5.6.1. Сроки обработки персональных данных определяются в соответствие со сроками действия договоров с субъектами персональных данных, а также требованиями законодательства и внутренних документов Общества.

5.7. Необходимость согласия субъекта на обработку персональных данных

5.7.1. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме. В случаях, предусмотренных федеральным законом, 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 к Положению.

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, который готовит ответственный за организацию обработки ПДн, определенный владельцем ИСПДн, и утверждает у руководителя Общества.

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, а также обязанность соблюдения требований к защите обрабатываемых персональных данных, указанных в соответствии со статьей 19 Федерального закона «О персональных данных».

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 внутренними документами Общества.

6.2.5. Сведения о работающем или уволенном работнике могут быть предоставлены третьим лицам (юридическим или физическим) 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 Российской Федерации, в следующих случаях и в сроки, установленные законодательством Российской Федерации:

- 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 такое согласие требуется в соответствии с законодательством Российской Федерации;
- при невозможности устранения допущенных нарушений при обработке персональных данных;
- при истечении срока действия согласия на обработку 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 положения.

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» определяются лица, ответственные за организацию обработки ПДн.

7.1.4. Для выбора и реализации методов и способов защиты персональных данных могут привлекаться организации, имеющие оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

7.1.5. Порядок формирования списка лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим им для выполнения должностных обязанностей, определяется в СТП «Управление доступом к информационным ресурсам информационных систем». 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 «Аудит информационной безопасности».

7.1.8. Процедуры (которые предусматривают документальную фиксацию результатов проводимых проверок) приема на работу, влияющие на обеспечение информационной безопасности, включают:

- 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 положении 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 в Обществе в соответствии с:

- базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России 15 февраля 2008 г.;
- методикой оценки угроз безопасности информации, утвержденной ФСТЭК России 05 февраля 2021 г.;
- 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»;
- положениями 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), определяет уровень защищенности ИСПДн, вносит всю необходимую информацию в акт классификации ИСПДн (Приложение 4), при этом Подразделение ИБ может привлекаться для консультаций;
- владелец ИСПДн назначает ответственного за организацию обработки ПДн;
- ответственный за организацию обработки ПДн направляет акт классификации ИСПДн руководителю ИТ службы;
- руководитель ИТ службы назначает ответственного работника для заполнения технической информации в акте классификации ИСПДн;
- ответственный за организацию обработки ПДн выносит акт классификации ИСПДн для его рассмотрения владельцем ИСПДн и утверждения руководителем Общества;
- по результатам рассмотрения акта классификации ИСПДн руководитель Общества 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 организацию обработки ПДн 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. № 687.

7.3.2. Обработка персональных данных 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 такой обработки ими персональных данных, 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.

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. Рекомендуемая структура модели угроз берётся из методики оценки угроз безопасности информации, утвержденной ФСТЭК России 05 февраля 2021 г.

7.5.1. Если по результатам исполнения п. 7.2 система остается ИСПДн, то ответственным за организацию обработки ПДн 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 её ответственному за организацию обработки ПДн;
- ответственный за организацию обработки ПДн направляет частную модель угроз ИСПДн руководителю ИТ службы, а тот назначает ответственного работника для заполнения технической информации;
- ответственный работник ИТ службы заполняет частную модель угроз ИСПДн (Приложение 5; пункты 4.5-4.11; Таблица 2) и направляет ответственному за организацию обработки ПДн;
- ответственный за организацию обработки ПДн предоставляет частную модель

угроз ИСПДн экспертной комиссии, в составе которой должны быть представители владельца ИСПДн, ИТ службы, защиты ресурсов и Подразделения ИБ для экспертной оценки угроз информационной безопасности;

- экспертная комиссия уточняет перечень угроз и определяет возможность реализации угроз и опасность каждой угрозы, эти данные формируются ответственным за организацию обработки ПДн и вносятся в частную модель угроз ИСПДн;
- по окончании работы экспертной комиссии ответственный за организацию обработки ПДн рассчитывает показатели и определяет актуальные угрозы безопасности ПДн;
- ответственный за организацию обработки ПДн выносит на рассмотрение владельца ИСПДн окончательный вариант частной модели угроз ИСПДн, по результатам рассмотрения принимается решение о ее утверждении у руководителя Общества или её доработке;
- копия частной модели угроз ИСПДн возвращается владельцу ИСПДн для хранения.

7.6. Подготовка плана мероприятий по обеспечению безопасности ИСПДн

7.6.1. Ответственный за организацию обработки ПДн при участии профильных подразделений Общества (кадровая служба, юридическая служба, Подразделение ИБ, ИТ служба и проч.) подготавливает план мероприятий по обеспечению безопасности ИСПДн с указанием ответственных за мероприятия исполнителей, в соответствии с СТП «Политика 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 ответственному за организацию обработки ПДн для утверждения руководителем Общества.

7.6.3. Ответственный за организацию обработки ПДн направляет утвержденный план мероприятий по обеспечению безопасности ИСПДн владельцу ИСПДн.

7.6.4. В рамках исполнения требований информационной безопасности владелец ИСПДн выпускает приказ о реализации мероприятий по защите персональных данных в ИСПДн и направляет утвержденный план мероприятий по обеспечению безопасности ответственным за мероприятия исполнителям и в Подразделение ИБ.

7.6.5. Ответственные за мероприятия исполнители присылают отчеты о выполнении мероприятий ответственному за организацию обработки ПДн.

7.6.6. Ответственный за организацию обработки ПДн после получения отчетов по всем мероприятиям плана направляет их владельцу ИСПДн для рассмотрения. Подразделение ИБ может привлекаться для экспертизы выполненных мероприятий.

7.6.7. Руководитель Общества 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. Ответственный за организацию обработки ПДн готовит протокол по результатам рассмотрения о степени соответствия мер защиты ПДн заданным требованиям по безопасности в виде деклараций о соответствии ИСПДн в форме акта соответствия (Приложение 6).

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

8. Права и обязанности работников Общества

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

8.2. 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.

8.3. Работник обязан:

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

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

9. Ответственные за организацию обработки персональных данных. Контроль за выполнением требований

9.1. Владельцы ИСПДн обязаны своевременно и качественно определить необходимые и достаточные сведения по обработке ПДн.

9.2. Ответственные за организацию обработки ПДн назначаются владельцами ИСПДн посредством издания приказа.

9.3. Обязанности ответственного за организацию обработки ПДн:

- организация и координация мероприятий по защите персональных данных в ИСПДн согласно разделу 7 настоящего положения;
- 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, внутренних документов по вопросам обработки персональных данных, требований к защите персональных данных;
- организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов;
- ведение журнала нештатных ситуаций (Приложение 2), внесение в него соответствующих записей в случае обнаружения фактов несоблюдения условий хранения носителей персональных данных либо использования средств обработки информации, которое может привести к нарушению конфиденциальности персональных данных или другим нарушениям.

9.4. Ответственные за организацию обработки ПДн имеют право на:

- привлечение к проведению работ по защите персональных данных работников других подразделений Общества;
- привлечение к проведению работ по защите персональных данных на договорной основе сторонних организаций;
- создание экспертных комиссий для выполнения мероприятий по защите персональнчых данных;
- запрос и получение необходимых материалов для организации и проведения

работ по вопросам обеспечения безопасности персональных данных в Обществе;

- контроль деятельности структурных подразделений Общества в части выполнения ими требований по обеспечению безопасности персональных данных.

9.5. Работники, привлечённые для осуществляющие функции по защите персональных данных, имеют право на:

- запрос и получение необходимых материалов для проведения работ по вопросам обеспечения безопасности персональных данных в Обществе.

9.6. Работники Подразделения ИБ имеют право на проведение выборочного контроля исполнения требований настоящего положения в соответствии с порядком, установленным СТП «Аудит информационной безопасности».

9.7. Для проверки выполнения требований положения приказом Общества могут быть созданы соответствующие комиссии.

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

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

10. Ответственность

10.1. Ответственность за осуществление контроля выполнения требований настоящего положения, предоставление рекомендаций по их выполнению, а также за поддержание данного документа в актуальном состоянии несет руководитель Подразделения ИБ.

10.2. 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.

10.3. Владельцы ИСПДн несут ответственность за своевременное определение факта обработки ПДн, подготовку сведений для классификации информационной системы и назначение ответственного за организацию обработки ПДн в своей ИСПДн.

10.4. Ответственные за организацию обработки персональных данных, а также работники, привлечённые для осуществления функции по защите персональных данных, несут ответственность за:

- правильность и адекватность принимаемых решений по защите персональных данных;
- качество проводимых работ и выполнение возложенных на них обязанностей, предусмотренных настоящим положением.

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

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

Приложение 1

От_____

_____

(Ф.И.О. полностью)

Согласие на передачу и обработку персональных данных

Я, (ФИО полностью) _____

_____

*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 *Акционерному обществу «ЭнСер»,* далее – Оператор, адрес *г. Миасс, пр. Автозаводцев 1*: 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 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 АО «ЭнСер»;
- 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 рождения, место рождения, гражданство, пол;
- прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- данные паспорта (сери я, номер, кем и когда выдан, номер подразделения);
- данные загранпаспорта (серия, номер, срок действия);
- адрес регистрации по месту жительства и фактического проживания;
- дата регистрации по месту жительства;
- номер телефона (домашний, мобильный, корпоративный);
- адрес личной электронной почты (e-mail);
- владение иностранными языками и языками народов Российской Федерации;
- должность и место работы, профессия, структурное подразделение;
- сведения о трудовом стаже;
- выполняемая работа с начала трудовой деятельности (включая военную службу);
- сведения о воинском учете;
- состояние в браке, сведения о составе семьи (ближайшие родственники);
- сведения об усыновлении (удочерении);
- 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);
- сведения по повышению квалификации и переподготовки работников, их аттестации;
- государственные награды, иные награды и знаки отличия (кем награжден и когда);
- сведения о планируемом отпуске;
- сведения о социальных льготах;
- индивидуальный номер налогоплательщика (ИНН);
- номер страхового свидетельства обязательного пенсионного страхования (СНИЛС);
- условия налоговых вычетов;
- реквизиты банковских счета и карты, указанные для выплаты заработной платы и иных денежных средств, причитающихся в процессе трудовой деятельности;
- система оплаты труда, должностной оклад (часовая ставка), сведения о доходах;
- график работы;
- данные водительского удостоверения (серия, номер, категория, дата выдачи, срок действия, стаж вождения);

- номер избирательного участка.

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 **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, для отражения и учета взаиморасчетов между Работником и Оператором **ООО «УСЦ «ЕвроСибЭнерго» (адрес:, г. Иркутск, ул. Бурлова, дом 2, офис. 408) ,** **ООО «Эн+ Диджитал» (адрес: г. Иркутск, Нижняя Набережная улица, дом 14/1)**	Фамилия, имя, отчество Дата 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 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 трудовом 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 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 **- Ингосстрах Банк адрес: г. Москва, Сущевская ул., 27, стр. 1;** **-ПАО «Сбербанк» адрес: г. Москва, 117997, ул. Вавилова, д. 19;** **- либо иному банку, указанному в заявлении работника.**	Фамилия, имя, отчество Дата рождения Паспортные данные Адрес регистрации и фактического места жительства	
Страховой компании – для оформления страховых случаев, страховых рисков в результате несчастного случая с Работниками **-СПАО «Ингосстрах» (адрес: г. Москва, ул. Пятницкая, д. 12, стр. 2);** **-ООО «СК «Ингосстрах-Жизнь» (адрес: г. Москва, Ленинградское шоссе, д.16, стр.9)**	Фамилия, имя, отчество Дата рождения	
Компании, оказывающей типографские и издательские услуги – для оформления	Фамилия, имя, отчество Структурное подразделение Должность	

визитных карточек, изготовления табличек на двери, издания корпоративной газеты **-ООО «Социальный комплекс» (адрес: г. Миасс, пр. Автозаводцев д.1 оф 441);** **- ООО «Абориген» (адрес: г. Миасс, пр. Макеева, 24- 47).**	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 **- АО «Аэроклуб»** **(адрес: г. Москва, 3-я Рыбинская ул., д.18, стр.22);** **- либо иному агентству по договору.**	Фамилия, имя, отчество Дата рождения Паспортные данные, в том числе заграничного паспорта Гражданство Адрес регистрации и фактического места жительства Номер телефона	
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 рождения Структурное подразделение Должность/профессия или вид работ Стаж работы Дата устройства на работу	
Учебным центрам и организациям – для организации обучения, участия в семинарах, конференциях: **- АНО ДПО Учебный центр ТехСервис** адрес: **Челябинская обл., г. Миасс, Тургоякское шоссе, 3/12;** **- ООО «Центр подготовки специалистов «Сварка и контроль» адрес: г. Челябинск, ул. Рылеева, д. 11;** **- АНО ДПО Учебный центр «Перспектива» адрес: Челябинск, пр. Победы, 160;** **- ООО «ВнешЭкономАудит.Консалтинг» адрес: г. Челябинск, ул. Красная, д.63;** **- МГО ЧО ООО "ВДПО"** адрес: **г. Миасс, Октябрьская ул, 29 и другие организации;** **- либо иному Учебному центру по заключенному договору.**	Фамилия, имя, отчество Дата 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 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 **- Министерство энергетики Российской Федерации адрес: г. Москва, Китайгородский проезд д. 7;** **- Администрация Миасского городского округа адрес: г. Миасс, проспект Автозаводцев, 55;** **-Правительство Челябинской области адрес: г. Челябинск, ул. Цвиллинга, 27;** **- Законодательное собрание Челябинской области г. адрес: Челябинск, ул. Кирова, д. 114;** **-Министерство тарифного регулирования и энергетики Челябинской области адрес: г. Челябинск, ул. Сони Кривой, д.75 .**	Фамилия, имя, отчество Дата 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 СНИЛС Страховое свидетельство	
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 Дата 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 дата рождения, 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 Стаж работы	
Размещение информации на корпоративных Интернет-ресурсах, либо иному печатному изданию **- сайт АО «ЭнСер»;** **- сообщество VK страница АО «ЭнСер»;** **- Telegram АО «ЭнСер»;**	Фамилия, имя, отчество Должность Фото Учебные заведения, в которых работник учился, периодов учебы, ученая степень Дата трудоустройства Стаж работы в данной области	

- в электронных, печатных, телевизионных, городских, региональных и федеральных СМИ.	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	
Приобретение путевок в санаторно-курортные организации, оздоровительные учреждения; приобретение путевок в Детские оздоровительные лагеря для детей работников: **- Управление Профтур Федерации профсоюзов Челябинской области адрес 454091, Челябинск, ул.Цвиллинга, 46;** **- ООО «Социальный комплекс» адрес: г. Миасс. пр. Автозаводцев 1;** **- либо иному Контрагенту, указанному в заявлении работника**	Фамилия, имя, отчество дата рождения Паспортные данные Адрес регистрации и фактического места жительства Номер телефона	

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
Положением об обработке и защите персональных данных работников АО «ЭнСер» я ознакомлен(а).

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)

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

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

Приложение 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 работников оператора, если в ней обрабатываются персональные данные только указанных работников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся работниками 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 работниками 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 работников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся работниками 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 работниками 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 работниками 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 работниками 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 работников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся работниками оператора;

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

в) для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает специальные категории персональных данных работников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся работниками 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 работниками 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 работников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся работниками 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), ответственное 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 работника 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	Работники 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

УТВЕРЖДАЮ
Руководитель Общества
«____» _____ 202_ 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 работники оператора/не являющихся работниками оператора.

Информационная система является информационной системой, обрабатывающей персональные данные работников оператора, если в ней обрабатываются персональные данные только указанных работников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся работниками 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 г. №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-1/2/3/4.

«_____»_____202_ г.
Председатель комиссии _____ _____
Члены комиссии
_____ _____
_____ _____
_____ _____

Приложение 5

УТВЕРЖДАЮ
Руководитель Общества

«____» _____ 202_ г.

Частная модель угроз
безопасности персональных данных
в информационной системе персональных данных
«Наименование ИСПДн»

Оглавление

1. Общие положения

1.1. Назначение и область действия документа.
Документ описывает актуальные угрозы ИСПДн «Наименование ИСПДн». На основании его строится защита, выбираются необходимые меры.
1.2. Владелец ИСПДн.
Владельцем информационной системы персональных данных «Наименование ИСПДн» является <заместитель генерального директора>.
1.3. Цель обработки персональных данных и её обоснование. Назначение, задачи (функции) системы, основные бизнес-процессы.
<Регистрация сведений, необходимых для осуществления Обществом уставной деятельности>
Указанные выше цели выполняются на основании следующих нормативно-правовых актов: Трудовой кодекс, требования по охране труда и т.д.
Создание данной ИСПДн позволяет автоматизировать процесс обработки персональных данных работников при их устройстве на работу, расчету заработной платы, оформления отпусков и проч.
1.4. 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.
1.5. Перечень действий с персональными данными и способы их обработки.
Оператором совершаются сбор, запись, хранение, уточнение. Ведется смешанная обработка ПДн.
1.6. Документы, используемые для оценки угроз безопасности информации и разработки модели угроз.
Угрозы взяты из банка данных угроз безопасности информации ФСТЭК, данных внутреннего аудита ИБ, ATT&CK, OWASP.
1.7. Уровень защищенности ИСПДн определён как УЗ-1/2/3/4
1.8. Привлекаемые для разработки модели угроз специалисты и организации.
Для разработки этой модели угроз была собрана экспертная группа работников подразделений владельца ИСПДн, кадровой службы, юридической службы, ИТ службы и Подразделения ИБ.

2. Описание систем и сетей и их характеристика как объектов защиты.

2.1. Условия расположения основных составляющих АС, обрабатывающих персональные данные.
2.1.1. 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: _____.
2.1.2. Границы контролируемых зон.
Контролируемыми зонами являются здания в которых располагаются структурные единицы.
2.2. Топология ИСПДн и конфигурация ее отдельных компонентов.
2.2.1. Топология ИСПДн.
Основными составляющими ИСПДн являются:
- центральный узел обработки данных;
- узел администрирования;
- автоматизированные рабочие места (АРМ) работников.

2.3. Конфигурация отдельных компонентов ИСПДн.

2.3.1. 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.

2.3.2. Узел администрирования.

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

2.3.3. АРМ работников.

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

АРМ работников установлено в зданиях ИД, Ф и ДО.

2.4. Связи между основными компонентами ИСПДн.

2.4.1. 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 (Интернет);
- узел администрирования подключен в локальную сеть ИД.

2.4.2. 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.

2.4.3. Функциональные связи.

Введенные на АРМ работников 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 работников;
- устанавливает политики безопасности, в соответствии с которыми АРМ работников получают возможность работать с центральным узлом обработки данных.

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

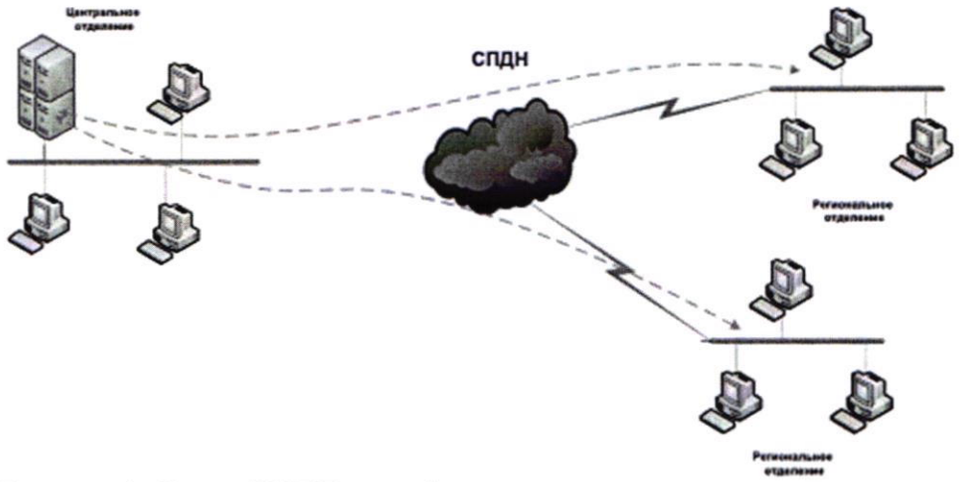


Рисунок 1. Схема ИСПДн и информационных потоков в ней.

2.5. Технические средства, участвующие в обработке персональных данных в ИСПДн.
В обработке персональных данных участвуют следующие технические средства:
- сервера HP;
- АРМ работников.
Кроме того, в обработке персональных данных участвует активное и пассивное сетевое оборудование производства Cisco: коммутаторы, межсетевые экраны, маршрутизаторы, модемы.
2.6. Общесистемные и прикладные программные средства, участвующие в обработке персональных данных.
В обработке персональных данных участвует следующее общесистемное программное обеспечение:
- ОС Windows 2003/2008/2012/XP/Vista/Windows7.
В обработке персональных данных участвует следующее прикладное программное обеспечение:
- ПО «Автоматизированная система v.1»;
- СУБД Oracle.
2.7. Режим и степень участия персонала в обработке персональных данных.
Обработка персональных данных во всех компонентах ИСПДн осуществляется в многопользовательском режиме.
2.7.1. 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.
2.7.2. 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.

3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

3.1. При реализации угроз безопасности информации возможно нарушение основных свойств информации: конфиденциальности, целостности, доступности.

3.2. Реализация угрозы может привести к нарушению прав субъектов ПДн и соответствующих законодательных актов. При этом может быть нанесен ущерб физическому лицу (выбрать из списка):

(Угроза жизни или здоровью. Унижение достоинства личности. Нарушение свободы, личной неприкосновенности. Нарушение неприкосновенности частной жизни. Нарушение личной, семейной тайны, утрата чести и доброго имени. Нарушение тайны переписки, телефонных переговоров, иных сообщений. Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности (утечка) персональных данных. «Травля» гражданина в сети «Интернет».)

3.3. Реализация угрозы может привести к нарушению работы сопутствующих бизнес-процессов Общества и реализации рисков, связанных с хозяйственной деятельностью Общества (выбрать из списка):

(Нарушение законодательства Российской Федерации. Потеря (хищение) денежных средств. Недополучение ожидаемой (прогнозируемой) прибыли. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Срыв запланированной сделки с партнером. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря клиентов, поставщиков. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Снижение престижа. Дискредитация работников. Утрата доверия. Причинение имущественного ущерба. Неспособность выполнения договорных обязательств. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). Принятие неправильных решений. Простой информационной системы или сети. Публикация недостоверной информации на веб-ресурсах организации. Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением. Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.))

3.4. Реализация угрозы может привести ущербу государству в обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности и нарушению соответствующих законодательных актов (выбрать из списка):

(Причинение ущерба жизни и здоровью людей. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения. Прекращение или

нарушение функционирования объектов транспортной инфраструктуры. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия). Прекращение или нарушение функционирования сети связи. Отсутствие доступа к государственной услуге. Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации. Снижение уровня дохода государственной корпорации, государственной организации или организации с государственным участием. Возникновение ущерба бюджетам Российской Федерации. Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций в системно значимой кредитной организации, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка. Вредные воздействия на окружающую среду. Прекращение или нарушение функционирования пункта управления (ситуационного центра). Снижение показателей государственного оборонного заказа. Прекращение или нарушение функционирования информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка. Нарушение законодательства Российской Федерации. Публикация недостоверной социально значимой информации на веб-ресурсах, которая может привести к социальной напряженности, панике среди населения и др. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов. Нарушение общественного правопорядка, возможность потери или снижения уровня контроля за общественным правопорядком. Нарушение выборного процесса. Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации. Организация пикетов, забастовок, митингов и других акций. Массовые увольнения. Увеличение количества жалоб в органы государственной власти или органы местного самоуправления. Появление негативных публикаций в общедоступных источниках. Создание предпосылок к внутриполитическому кризису. Доступ к персональным данным сотрудников органов государственной власти, уполномоченных в области обеспечения обороны, безопасности и правопорядка, высших должностных лиц государственных органов и других лиц государственных органов. Доступ к системам и сетям с целью незаконного использования вычислительных мощностей. Использование веб-ресурсов государственных органов для распространения и управления вредоносным программным обеспечением. Утечка информации ограниченного доступа. Не предоставление государственных услуг.).

4. Возможные объекты воздействия угроз безопасности информации

4.1. Объекты воздействия угроз указаны в разделе 2 модели угроз.

4.2. Основными видами воздействия на эти объекты являются:

- утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);
- несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;
- отказ в обслуживании компонентов (нарушение доступности);
- несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);
- несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;
- нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации.

4.3. Объекты воздействия должны быть защищены на всех уровнях модели взаимосвязи открытых систем (модель OSI) (от физического до прикладного).

4.4. Арендуемые или используемые на ином законном основании программно-аппаратные средства и их интерфейсы, каналы связи, программное обеспечение (в том числе программное обеспечение виртуализации и построенных на его базе виртуальных машин, виртуальных серверов, систем управления виртуализацией, виртуальных каналов связи и т.д.) относятся к объектам воздействия, находящимся в границе оценки угроз безопасности информации оператора. В отношении остальной информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры угрозы безопасности информации оцениваются поставщиком услуг. Оператор и поставщик услуг работают по схеме (выбрать): инфраструктура как услуга, платформа как услуга, программное обеспечение как услуга.

5. Источники угроз безопасности информации.

5.1. На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определены следующие виды нарушителей, актуальные для систем и сетей: специальные службы иностранных государств; террористические, экстремистские группировки; преступные группы (криминальные структуры); отдельные физические лица (хакеры); конкурирующие организации; разработчики программных, программно-аппаратных средств; лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем; поставщики услуг связи, вычислительных услуг; лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ; лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.); авторизованные пользователи систем и сетей; системные администраторы и администраторы безопасности; бывшие (уволенные) работники (пользователи).

5.2. Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителей по реализации угроз безопасности информации. В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:

- базовыми возможностями по реализации угроз безопасности информации (Н1);
- базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
- средними возможностями по реализации угроз безопасности информации (Н3);
- высокими возможностями по реализации угроз безопасности информации (Н4).

5.3. Для актуальных нарушителей определены их категории в зависимости от имеющихся прав и условий по доступу к системам и сетям, обусловленных архитектурой и условиями функционирования этих систем и сетей, а также от установленных возможностей нарушителей.

5.4. При этом нарушители подразделяются на две категории:

- внешние нарушители – нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;
- внутренние нарушители – нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

6. Способы реализации (возникновения) угроз безопасности информации.

6.1. На основе анализа исходных данных, а также возможностей нарушителей определяются способы реализации (возникновения) угроз безопасности информации, актуальные для

систем и сетей. Основными способами реализации (возникновения) угроз безопасности информации являются:

- использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей);
- внедрение вредоносного программного обеспечения;
- использование не декларированных возможностей программного обеспечения и (или) программно-аппаратных средств;
- установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;
- формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;
- перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
- инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
- нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);
- ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

6.2. Указанные способы реализации (возникновения) угроз безопасности информации могут быть дополнены иными способами с учетом особенностей архитектуры и условий функционирования систем и сетей.

6.3. Способы реализации (возникновения) угроз безопасности информации определяются применительно к объектам воздействия, определенным в соответствии с настоящей Моделью. Способы являются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз безопасности и имеются или созданы условия, при которых такая возможность может быть реализована в отношении объектов воздействия. Одна угроза безопасности информации может быть реализована несколькими способами.

6.4. Условием, позволяющим нарушителям использовать способы реализации угроз безопасности информации, является наличие у них возможности доступа к следующим типам интерфейсов объектов воздействия:

- внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
- внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы (проводные, беспроводные);
- интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
- интерфейсы для использования съемных машинных носителей информации и периферийного оборудования; интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей;
- возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей.

6.5. Наличие указанных интерфейсов определяется архитектурой, составом и условиями функционирования систем и сетей, группами пользователей, их типами доступа и уровнями полномочий. В ходе анализа должны быть определены как логические, так и

физические интерфейсы объектов воздействия, в том числе требующие физического доступа к ним.

6.6. Интерфейсы определяются на аппаратном, системном и прикладном уровнях систем и сетей, а также для телекоммуникационного оборудования. Возможность их использования на указанных уровнях определяется возможностями актуальных нарушителей.

6.7. На этапе создания систем и сетей определение интерфейсов объектов воздействия, которые могут использоваться для реализации угроз безопасности, проводится на основе предполагаемой архитектуры и условий функционирования систем и сетей, определенных на основе изучения и анализа исходных данных о них.

6.8. На этапе эксплуатации систем и сетей для определения интерфейсов объектов воздействия, которые могут использоваться для реализации угроз безопасности, дополнительно к документации на сети и системы используются результаты инвентаризации систем и сетей, проведенной с использованием автоматизированных средств.

6.9. По результатам оценки возможных способов реализации угроз безопасности информации должны быть определены: а) виды и категории нарушителей, которые имеют возможность использования актуальных способов; б) актуальные способы реализации угроз безопасности информации и типы интерфейсов объектов воздействия, за счет которых они могут быть реализованы.

7. Актуальные угрозы безопасности информации

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).

7.1. 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 работников организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	-
- ИСПДн, к которой имеют доступ все работники 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.

7.2. Определение вероятности реализации угроз в ИСПДн

Под вероятностью реализации угрозы поднимается определяемый экспертным путем показателя, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки и учётом негативных последствий.

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 нарушителями с различным уровнем возможностей (Hn) приведена в таблице 3.

Y2 берётся максимальной из всех по уровням возможностей Hn.

Таблица 3

Оценка вероятности реализации угрозы безопасности нарушителями с различным уровнем возможностей

Виды воздействия (способы реализации угроз) на ИСПДн	Объект воздействия	Доступные интерфейсы	Вероятность реализации угрозы нарушителем с уровнем возможностей Hn				
			H1	H2	H3	H4	Итог Y2

угрозы утечки акустической (речевой) информации	АРМ	Физическая среда	0	0	0	0	0
угрозы утечки видовой информации	АРМ	Монитор, клавиатура	5	0	0	0	2
угрозы утечки по каналу ПЭМИН	АРМ	Физическая среда	0	0	0	0	0
угрозы, реализуемые в ходе загрузки операционной системы	АРМ, Сервер	Порты ввода/вывода АРМ	0	0	0	0	0
угрозы, реализуемые после загрузки операционной системы	АРМ, Сервер	Операционная система, устройства ввода/вывода	0	2	2	2	2
угрозы внедрения вредоносных программ	АРМ, Сервер	Порты ввода/вывода	2	5	0	0	5
угрозы "Анализ сетевого трафика" с перехватом передаваемой по сети информации	Линия связи между сервером и АРМ	Каналы передачи данных	2	2	0	0	2
угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	БД ИС	Каналы передачи данных	2	2	0	0	2
угрозы типа "Отказ в обслуживании"	МЭ, коммутатор, сервер	Каналы передачи данных	2	2	0	0	2
угрозы выявления паролей	Линия связи между сервером и АРМ, сервер, АРМ	Каналы передачи данных, монитор, физическая среда	2	2	0	0	2
угрозы удаленного запуска приложений	АРМ, Сервер	Операционная система, устройства ввода/вывода	2	2	0	0	2
угрозы внедрения ложного объекта сети	Сеть	Каналы передачи данных	2	2	2	2	2
угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	МЭ, маршрутизатор, коммутатор	Каналы передачи данных	5	5	0	0	5
угрозы внедрения по сети вредоносных программ	АРМ, Сервер	Каналы передачи данных	2	2	0	0	2

7.3. 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:

$0 \leq Y \leq 0,3$ - низкая;
$0,3 < Y \leq 0,6$ - средняя;
$0,6 < Y \leq 0,8$ - высокая;
$Y > 0,8$ - очень высокая.

Таблица 4

Оценка возможность реализации угрозы

Виды воздействия (способы реализации угроз) на ИСПДн	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

7.4. Оценка опасности угроз в ИСПДн АС

Оценка опасности производится на основе опроса специалистов экспертной комиссии по ИСПДн, и определяется вербальным показателем опасности, который имеет 3 значения:
- низкая опасность – 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

Оценка опасности

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

7.5. 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

Правила определения актуальности угрозы

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

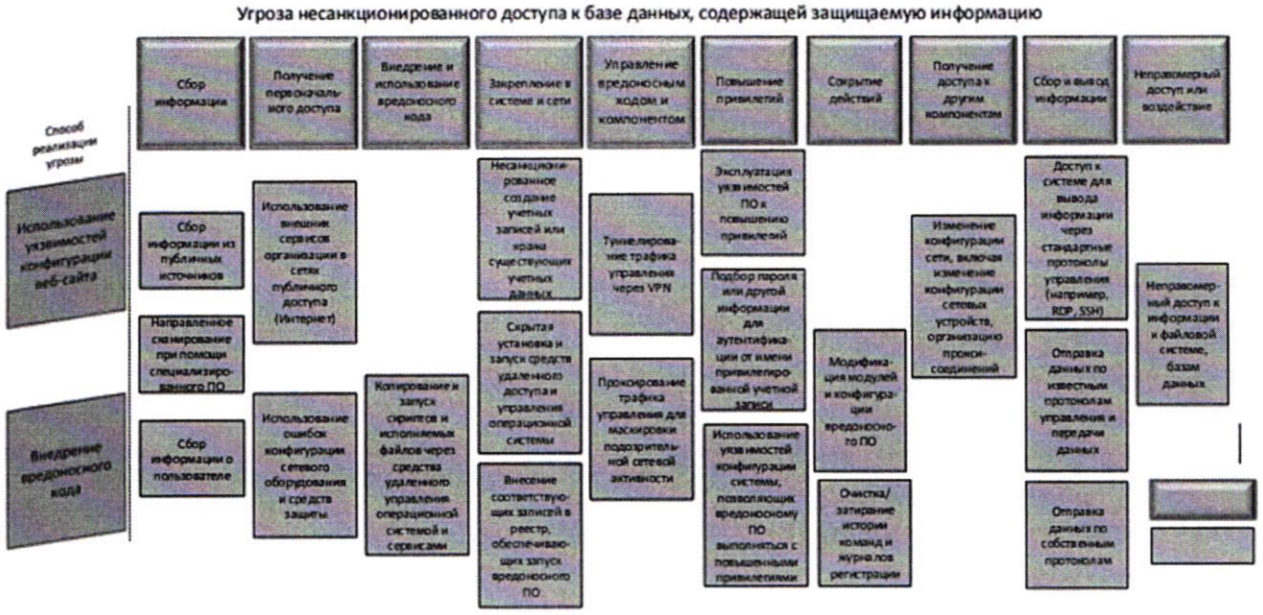
Актуальность угроз

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.

Для реализации указанных актуальных угроз возможны следующие сценарии:



Приложение 6

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

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

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