ПОЛИТИКА
обработки и обеспечения безопасности персональных данных в ПАО НК «РуссНефть»

Москва
2023

1. Общие положения

Политика обработки и обеспечения безопасности персональных данных (далее ПДн) в ПАО НК «РуссНефть» (далее Политика) является локальным нормативным актом ПАО НК «РуссНефть» (далее Компания), разработанным в соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и определяет основные принципы, цели и условия обработки ПДн, а также меры защиты ПДн в Компании.

Контроль за исполнением требований настоящей Политики осуществляется Ответственным за организацию обработки ПДн.

Настоящая Политика разработана в целях реализации требований законодательства Российской Федерации в области Обработки ПДн и обеспечения Безопасности ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Компания вправе вносить изменения в Политику с соблюдением требований законодательства Российской Федерации и нормативных правовых актов.

2. Термины и определения

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники.

Безопасность ПДн – состояние защищенности ПДн, при котором обеспечены их конфиденциальность, доступность и целостность.

Блокирование ПДн – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность ПДн – обязательное для выполнения лицом, получившим доступ к ПДн, требование не передавать такие ПДн третьим лицам без согласия ее обладателя.

Несанкционированный доступ (НСД) – доступ к ПДн или действия с ПДн, нарушающие правила разграничения доступа с использованием средств, предоставляемых ИСПДн.

Носитель ПДн – технические устройства, предназначенные для записи и обработки ПДн в составе средств вычислительной техники, а также для хранения и перемещения записанных ПДн за пределы состава средств вычислительной техники, а также бумажные носители ПДн.

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

Обработка ПДн без использования средств автоматизации – действие с ПДн, такие как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн, осуществляемое при непосредственном участии человека.

Ответственный за обеспечение безопасности ПДн – лицо, ответственное за обеспечение безопасности ПДн, за реализацию и непрерывность соблюдения установленных мер защиты и осуществляющее контроль функционирования средств защиты информации, применяемых в ИСПДн Компании.

Ответственный за организацию обработки ПДн – лицо, осуществляющее внутренний контроль за соблюдением Компанией и ее работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту ПДн).

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

Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Работник Компании – лицо, осуществляющее свою деятельность в Компании на основании трудового договора, и имеющее возможность получить доступ к обработке ПДн, как с применением автоматизированных средств обработки ПДн, так и без таковых.

Система защиты ПДн (СЗПДн) – комплекс организационных и технических мер, определенных с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.

Средства защиты информации (СЗИ) – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.

Субъект ПДн – физическое лицо, которое прямо или косвенно определено или определяемо с помощью ПДн.

Уполномоченный орган по защите прав субъектов ПДн – федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки ПДн требованиям законодательства Российской Федерации в области ПДн.

ФЗ «О персональных данных» – Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Иные термины, значение которых не определено в настоящей Политике, используются в значении, которое придается им законодательством Российской Федерации и нормативными правовыми актами.

3. Принципы обработки ПДн

Обработка ПДн Компанией осуществляется на основе принципов:

– законности и справедливости (соблюдения законодательных актов и соблюдения равноправных интересов Субъектов ПДн, не злоупотребляя представившимися возможностями на основании сведений, представленных Субъектом ПДн) целей и способов обработки ПДн;

– соответствия целей Обработки ПДн законным целям, заранее определенным и заявленным при сборе ПДн;

– соответствия объема и содержания обрабатываемых ПДн, способам и целям обработки ПДн;

– точности ПДн, их достаточности и актуальности по отношению к целям обработки ПДн;

– недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;

– недопустимости объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

– хранения ПДн в форме, позволяющей определить Субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, либо срок хранения ПДн, установленный законодательством Российской Федерации, договором, заключенным Компанией с Субъектом ПДн, согласием на обработку ПДн (далее – срок хранения ПДн);

– уничтожения ПДн по достижении целей их обработки, если срок хранения ПДн не установлен законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем, по которому является Субъект ПДн.

4. Цели и правовые основания обработки ПДн

Компания осуществляет сбор и Обработку ПДн в следующих целях:

– защиты жизни, здоровья или иных важных интересов субъектов ПДн;

– заключения, исполнения и прекращения гражданско-правовых договоров с физическими, юридическими лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных законодательством и Уставом Компании;

– организации кадрового учета, обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам;

– ведения кадрового делопроизводства, содействия работникам в трудоустройстве, обучении и кадровом перемещении в рамках штатного расписания, пользования различного вида льготами, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное

пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с Трудовым и Налоговым кодексами Российской Федерации, федеральными законами;

– организации и проведения практики, студентов по программам высшего профессионального обучения и среднего профессионального обучения;

– реализации контрольно-пропускного режима в Компании, обеспечения сохранности имущества;

– раскрытия информации об органах управления, ведение необходимой корпоративной и акционерной документации в соответствии с законодательством Российской Федерации;

– формирования справочных материалов для внутреннего информационного обеспечения деятельности Компании, ее филиалов, обществ, входящих в корпоративную структуру Компании, взаимозависимых юридических лиц;

– исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации;

– выдачи доверенностей представителям организаций, привлекаемых для реализации проектов деятельности Компании;

– совершения иных действий, не противоречащих законодательству Российской Федерации.

Основаниями для обработки ПДн Субъектов ПДн Компании, в том числе, являются:

– Гражданский кодекс Российской Федерации;

– Налоговый кодекс Российской Федерации;

– Трудовой кодекс Российской Федерации;

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

– Федеральный закон от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц»;

– Федеральный закон от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;

– Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;

– Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

– Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в

информационных системах персональных данных» (далее – Постановление Правительства РФ № 1119);

– Устав Компании.

В Компании осуществляется Автоматизированная обработка ПДн и Обработка ПДн без использования средств автоматизации путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (предоставления, предоставления, доступа), блокирования, удаления, уничтожения ПДн.

Компания в своей деятельности исходит из того, что при взаимодействии с Компанией Субъект ПДн предоставляет точную и достоверную информацию, о своих ПДн, а также своевременно извещает Компанию об изменении своих ПДн.

5. Категории ПДн и Субъектов ПДн

Компания обрабатывает ПДн следующих категорий Субъектов ПДн:

– работники;
– кандидаты на трудоустройство;
– контрагенты (физические лица, работники контрагентов);
– практиканты;
– работники сторонних организаций (в рамках договорных отношений);
– посетители Компании;
– члены Совета директоров.

В соответствии с положениями Постановления Правительства РФ № 1119 в Компании обрабатываются следующие категории ПДн без использования средств автоматизации и с использованием средств автоматизации:

– иные категории ПДн – ПДн, не отнесенные к категориям: специальные, биометрические и общедоступные ПДн;

– биометрические категории ПДн – сведения, которые характеризуют физиологические и биологические особенности человека.

Полный перечень ПДн и категории субъектов ПДн утверждается Перечнем обрабатываемых персональных данных.

6. Условия обработки ПДн Субъектов ПДн и условия передачи ПДн третьим лицам

Компания обрабатывает ПДн Субъектов ПДн в соответствии с локальными нормативными актами Компании, разработанными в соответствии с требованиями законодательства Российской Федерации в области ПДн.

Обработка ПДн в Компании допускается в следующих случаях:

– обработка ПДн осуществляется с согласия Субъекта ПДн на обработку его ПДн;

– обработка ПДн, разрешенных субъектом ПДн для распространения, осуществляется с согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, представляемого субъектом

персональных данных отдельно от других согласий субъекта персональных данных на обработку его ПДн;

– обработка ПДн необходима в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах; для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации;

– обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, является Субъект ПДн, а также для заключения договора по инициативе Субъекта ПДн;

– обработка ПДн осуществляется в статистических или иных исследовательских целях, за исключением случаев, установленных в ст. 15 ФЗ «О персональных данных», при условии обязательного обезличивания ПДн;

– осуществляется обработка ПДн, полученных из открытых источников, размещенных в них Субъектом ПДн либо по его просьбе;

– обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Если иное не предусмотрено федеральным законом, Компания вправе поручить обработку ПДн другому лицу, на основании заключаемого с этим лицом договора, при условии наличия согласия Субъекта ПДн. Лицо, осуществляющее обработку ПДн по поручению Компании, обязано соблюдать принципы и правила обработки ПДн, предусмотренные ФЗ «О персональных данных».

В поручении третьему лицу указываются цели обработки и перечень действий (операций) с ПДн, которые могут быть совершены данным лицом, устанавливается его обязанности по обеспечению Конфиденциальности ПДн и Безопасности ПДн при их обработке, а также требования к защите обрабатываемых ПДн в соответствии с ФЗ «О персональных данных».

Компания не осуществляет трансграничную передачу ПДн (передачу на территорию стран, обеспечивающих адекватную защиту ПДн с согласия субъекта ПДн).

Компанией не принимаются решения, порождающие юридические последствия в отношении Субъектов ПДн или иным образом затрагивающие их права и законные интересы, на основании исключительно Автоматизированной обработки ПДн, за исключением случая наличия согласия в письменной форме Субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов Субъекта ПДн.

Компания прекращает обработку ПДн в следующих случаях:

– при выявлении неправомерной Обработки ПДн, осуществляемой Компанией или лицом, действующим по поручению Компании. Компания в срок, не превышающий трех рабочих дней с даты такого выявления, прекращает неправомерную Обработку ПДн или обеспечивает прекращение неправомерной Обработки ПДн лицом, действующим по поручению Компании, и устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений Компания в срок, не превышающий десяти рабочих дней с даты

выявления неправомерности действий с ПДн, уничтожает ПДн или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Компания уведомляет Субъекта ПДн или его представителя, а в случае, если обращение или запрос были направлены в уполномоченный орган по защите прав Субъектов ПДн, также этот орган;

– при достижении цели Обработки ПДн Компания прекращает Обработку ПДн или обеспечивает ее прекращение (если Обработка ПДн осуществляется другим лицом, действующим по поручению Компании) и уничтожает ПДн или обеспечивает их уничтожение (если Обработка ПДн осуществляется другим лицом, действующим по поручению Компании) в срок, не превышающий тридцати дней с даты достижения цели Обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн, иным соглашением между Компанией и Субъектом ПДн либо если Компания не вправе осуществлять Обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных ФЗ «О персональных данных» или другими федеральными законами.

– при отзыве Субъектом ПДн согласия на обработку своих ПДн Компания прекращает обработку ПДн или обеспечивает ее прекращение (если Обработка ПДн осуществляется другим лицом, действующим по поручению Компании) и в случае, если сохранение ПДн более не требуется для целей Обработки ПДн, уничтожает ПДн или обеспечивает их уничтожение (если Обработка ПДн осуществляется другим лицом, действующим по поручению Компании) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн, иным соглашением между Компанией и Субъектом ПДн либо если Компания не вправе осуществлять Обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных ФЗ «О персональных данных» или другими федеральными законами.

В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в настоящем разделе, Компания осуществляет блокирование таких ПДн или обеспечивает их блокирование (если Обработка ПДн осуществляется другим лицом, действующим по поручению Компании) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7. Согласие на обработку ПДн

Получение и Обработка ПДн в случаях, предусмотренных ФЗ «О персональных данных», осуществляется Компанией с согласия Субъекта ПДн. Согласие на Обработку ПДн может быть дано Субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на Обработку ПДн от представителя Субъекта ПДн полномочия данного представителя на дачу согласия от имени Субъекта ПДн проверяются Компанией.

В случаях, предусмотренных ФЗ «О персональных данных», Обработка ПДн осуществляется Компанией только с согласия в письменной форме Субъекта ПДн.

Равнозначным содержащему собственноручную подпись Субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Письменное согласие Субъекта ПДн должно включать:

– фамилию, имя, отчество, адрес Субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

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

– наименование и адрес Компании;

– цель обработки ПДн;

– перечень ПДн, на обработку которых дается согласие Субъекта ПДн;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Компании, если Обработка ПДн поручена такому лицу;

– перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Компанией способов обработки ПДн;

– срок, в течение которого действует согласие, а также способ его отзыва, если иное не установлено федеральным законом;

– подпись Субъекта ПДн.

Субъект ПДн дает Компании согласие на Обработку ПДн свободно, по своей воле и в своем интересе. Согласие на обработку ПДн может быть отозвано Субъектом ПДн путем направления в Компанию письменного заявления в свободной форме. В этом случае Компания обязуется прекратить обработку, а также уничтожить все имеющиеся в Компании ПДн в сроки, установленные ФЗ «О персональных данных».

Передача ПДн третьим лицам осуществляется Компанией с согласия Субъекта ПДн в соответствии с требованиями законодательства Российской Федерации.

Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, оформляется отдельно от иных согласий субъекта ПДн на обработку его ПДн. Требования к содержанию согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, устанавливаются уполномоченным органом по защите прав субъектов персональных данных.

8. Права Субъектов ПДн

Для обеспечения соблюдения установленных законодательством прав Субъектов ПДн, в Компании разработан и введен порядок работы с обращениями и запросами Субъектов ПДн, а также порядок предоставления Субъектам ПДн информации, установленной законодательством Российской Федерации в области ПДн.

Субъект ПДн или его законный представитель имеет право на получение информации, касающейся Обработки ПДн, в том числе содержащей:

– подтверждение факта Обработки ПДн Компанией;
– правовые основания и цели Обработки ПДн;
– цели и применяемые Компанией способы обработки ПДн;
– наименование и местонахождение Компании, сведения о лицах (за исключением работников Компании), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Компанией или на основании федерального закона;
– обрабатываемые ПДн, относящиеся к соответствующему Субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
– сроки обработки ПДн, в том числе сроки их хранения;
– порядок осуществления Субъектом ПДн прав, предусмотренных ФЗ «О персональных данных»;
– информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
– наименование или фамилию, имя, отчество и адрес лица, осуществляющего Обработку ПДн по поручению Компании, если обработка поручена или будет поручена такому лицу;
– иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами в области ПДн.

Компания предоставляет указанную информацию при обращении или на основании соответствующего письменного запроса Субъекта ПДн или его представителя, содержащего: номер основного документа, удостоверяющего личность Субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие Субъекта ПДн в отношениях с Компанией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт Обработки ПДн Компанией, подпись Субъекта ПДн или его представителя.

Субъект ПДн вправе требовать от Компании уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели Обработки ПДн, а также принимать предусмотренные законодательством Российской Федерации в области ПДн меры по защите своих прав.

Для реализации и защиты своих прав и законных интересов в части обеспечения правомерности Обработки ПДн и обеспечения Безопасности ПДн Субъект ПДн имеет право обратиться к Компании.

Если Субъект ПДн считает, что Компания осуществляет Обработку ПДн с нарушением требований ФЗ «О персональных данных» или иным образом нарушает его права и свободы, Субъект ПДн вправе обжаловать действия или бездействие Компании в Уполномоченный орган по защите прав Субъектов ПДн или в судебном порядке.

Право Субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе, если доступ Субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

9. Права и обязанности Компании

Компания вправе:

– отстаивать свои интересы в судебных органах;

– предоставлять ПДн Субъектов третьим лицам, если это предусмотрено законодательством Российской Федерации (правоохранительные, налоговые органы и др.);

– отказывать в предоставлении ПДн в случаях, предусмотренных законодательством Российской Федерации;

– использовать ПДн Субъекта ПДн без его согласия, в случаях, предусмотренных законодательством Российской Федерации.

Обязанности Компании:

– обеспечивать Конфиденциальность в отношении ПДн, ставших известными Компании в ходе осуществления им своей деятельности;

– в случае выявления неправомерной Обработки ПДн, выявления неточных ПДн, при обращении Субъекта ПДн или его представителя либо по запросу Субъекта ПДн или его представителя осуществлять блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) с момента такого обращения;

– в случае достижения цели обработки ПДн прекращать Обработку ПДн или обеспечивает ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании) и уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Компании).

10. Обеспечение безопасности ПДн

Для обеспечения Безопасности ПДн Компания принимает необходимые и достаточные организационные и технические меры для защиты ПДн Субъектов ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий, включающие, в том числе:

– назначение приказом Компании Ответственного за организацию обработки ПДн и Ответственного за обеспечение безопасности ПДн, а также определение их функций и полномочий;

– разработка и поддержание в актуальном состоянии внутренних нормативных документов Компании в отношении Обработки ПДн и обеспечения Безопасности ПДн, установления процедур, направленных на выявление и

предотвращение нарушения в Компании законодательства Российской Федерации в области ПДн, устранения последствий таких нарушений;

– периодический внутренний контроль, а также контроль, осуществляемый сторонними организациями (внешний аудит) по договору подряда или оказания услуг, соответствия Обработки ПДн требованиям ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам;

– проведение оценки вреда, который может быть причинен Субъектам ПДн в случае нарушения законодательства о области ПДн, а также соотношение указанного вреда с принимаемыми мерами по обеспечению исполнения законодательства в области ПДн;

– ознакомление Работников Компании, непосредственно осуществляющих Обработку ПДн, с положениями законодательства Российской Федерации и внутренних нормативных документов Компании в отношении Обработки ПДн и обеспечению Безопасности ПДн, обучение указанных Работников Компании;

– определение угроз Безопасности ПДн при их обработке в ИСПДн;

– применение организационных и технических мер по обеспечению Безопасности ПДн при Обработке ПДн в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Постановлением Правительства РФ № 1119 уровни защищенности ПДн;

– применение прошедших в установленном порядке процедуру оценки соответствия СЗИ;

– оценка эффективности принимаемых мер по обеспечению Безопасности ПДн до ввода в эксплуатацию ИСПДн;

– учет Работников Компании, допущенных к обработке ПДн;

– учет материальных Носителей ПДн;

– обнаружение фактов НСД к ПДн и принятием мер;

– восстановление ПДн, модифицированных или уничтоженных вследствие НСД к ним;

– установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

– контроль за принимаемыми мерами по обеспечению Безопасности ПДн и уровня защищенности ИСПДн;

– определение порядка отнесения информационных систем к информационным системам персональных данных на основании утвержденных критериев;

– определение уровня защищенности ПДн для каждой ИСПДн;

– реализация в каждой ИСПДн системы идентификации и аутентификации, разграничения прав доступа и регистрации действий пользователей ИСПДн;

– реализация для каждой ИСПДн системы резервного копирования информации;

– применение систем антивирусной защиты и межсетевых экранов для защиты ИСПДн;

Комплекс мероприятий, предусмотренных Постановлением Правительства РФ № 1119 и приказом ФСТЭК России 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», по обеспечению Безопасности ПДн в Компании определяется в локальных нормативных актах Компании, с учетом результатов оценки возможного вреда Субъекту ПДн, который может быть нанесен в случае нарушения Безопасности его ПДн, актуальности угроз Безопасности ПДн, а также установления уровня защищенности ПДн.

11. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Компании в области ПДн

Внутренний контроль за соблюдением в Компании требований законодательства Российской Федерации и внутренних нормативных документов Компании в области ПДн осуществляется Ответственным за организацию обработки ПДн на постоянной основе с привлечением Ответственного за обеспечение безопасности ПДн.

Ответственный за организацию обработки ПДн, в частности, обязан:

– осуществлять внутренний контроль за соблюдением Компанией и Работниками Компании законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

– доводить до сведения работников Компании положения законодательства Российской Федерации о ПДн, внутренних нормативных документов Компании по вопросам Обработки ПДн, требований к защите ПДн;

– организовывать прием и обработку обращений и запросов Субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

12. Порядок действий при обнаружении утечки ПДн

Работник Компании обязан незамедлительно уведомить Ответственного за обеспечение безопасности ПДн о ставшем ему известном, готовящемся или свершившемся факте утечки ПДн при помощи корпоративной электронной почты или рабочего телефона.

Уведомление об утечке ПДн должно содержать сведения об источнике получения информации, дате и времени события, информацию о категориях ПДн и информационных системах ПДн, из которых произошла утечка ПДн и иные обстоятельства, известные работнику.

Ответственный за обеспечение безопасности ПДн незамедлительно осуществляет предварительный анализ обстоятельств, сообщенных работником и в случае, если факт утечки подтвержден, незамедлительно:

– информирует руководство Компании о случившемся факте;

– инициирует проведение проверки с привлечением заинтересованных подразделений Компании;

– выявляет предполагаемые причины утечки ПДн;

– проводит оценку предполагаемого вреда, нанесенного правам субъектов ПДн.

В срок не позднее 24 часов с момента выявления утечки ПДн Ответственный за обеспечение безопасности ПДн уведомляет Роскомнадзор о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий утечки ПДн, а также предоставляет сведения о лице, уполномоченном Компанией на взаимодействие с Роскомнадзором по вопросам, связанным с выявленным фактом утечки ПДн.

По результатам проведения проверки по факту утечки ПДн Ответственный за обеспечение безопасности ПДн не позднее 72 часов с момента выявления утечки ПДн уведомляет Роскомнадзор о результатах проверки, а также предоставляет сведения о лицах, действия которых стали его причиной (при наличии таковых).

13. Ответственность за реализацию положений Политики

Работники Компании, осуществляющие обработку ПДн, а также Ответственный за организацию обработки ПДн, Ответственный за обеспечение безопасности ПДн несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации за нарушение требований настоящей Политики, иных локальных нормативных актов Компании в области ПДн и законодательства Российской Федерации в области ПДн.