Политика в отношении персональных данных

**ПОЛОЖЕНИЕ
по организации и порядку проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
ООО «ГОРОДСКОЙ ЭКОЛОГИЧЕСКИЙ ЦЕНТР+»**

**1. Термины и определения**

персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

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;

блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

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;

обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

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

трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

угроза или опасность утраты персональных данных – единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

**2. Общие положения**

2.1. Настоящее положение разработано на основе Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781.

2.2. Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия. Для защиты ПДн создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

Мероприятия по обеспечению безопасности ПДн формулируются в зависимости от класса ИСПДн, определяемого с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства.

2.3. Для обеспечения безопасности ПДн при их обработке в ИСПДн осуществляется защита информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в ИСПДн.

2.4. Для защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют работы с персональными данными;

- строгое избирательное и обоснованное распределение документов и информации между работниками;

- рациональное размещение рабочих мест, при котором исключалось бы бесконтрольное использование защищаемой информации;

- знание сотрудниками предприятия требований нормативно-методических документов по защите информации;

- наличие необходимых условий в помещениях для работы с конфиденциальными документами и базами данных;

- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещения, в которых функционируют ИСПДн;

- организация порядка уничтожения информации;

- своевременное выявление нарушений требований разрешительной системы доступа к ПДн;

- обучение сотрудников, воспитательная и разъяснительная работа по вопросам информационной безопасности;

- определение и регламентация состава сотрудников, имеющих право доступа к информационным ресурсам ИСПДн.

**3. Основные мероприятия по организации обеспечения безопасности персональных данных**

3.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

3.2. Обязанности по реализации необходимых организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, возлагаются на ООО «ГОРЭКОЦЕНТР+» как оператора, осуществляющего обработку персональных данных.

3.3. Ответственным за обеспечение безопасности ПДн при их обработке в ИСПДн ООО «ГОРЭКОЦЕНТР+» назначен заместителя директора по общим вопросам. Функции по разработке и осуществлению мероприятий по организации и обеспечению безопасности ПДн возложены на заместителя директора по общим вопросам.

3.4. Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

3.5. Обработка персональных данных должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;

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

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

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

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

3.6. Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы (подсистемы) защиты персональных данных (СЗПДн). Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации, а также используемые в информационной системе информационные технологии.

3.7. Сотрудники предприятия, ответственные за хранение персональных данных, а также сотрудники предприятия, владеющие персональными данными в силу своих должностных обязанностей, подписывают Обязательство о конфиденциальности (Приложение 1).

3.8. Помещения, в которых хранятся и обрабатываются персональные данные, должны быть оборудованы надежными замками и сигнализацией на вскрытие помещений, в рабочее время данные помещения при отсутствии в них работников должны быть закрыты, проведение уборки помещений должно производиться в присутствии работников подразделений, ответственных за данные помещения.

**4. Обязанности должностных лиц, эксплуатирующих ИСПДн, в части обеспечения безопасности персональных данных при их обработке в ИСПДн**

4.1. При обработке персональных данных предприятие, выполняя функции оператора ПДн, обязано соблюдать следующие требования:

- обработка персональных данных осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;

- обработка персональных данных сотрудников предприятия осуществляется в целях содействия сотруднику в обучении и должностном росте, обеспечения личной безопасности сотрудника и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества предприятия, учета результатов исполнения им должностных обязанностей;

- персональные данные следует получать лично у субъекта ПДн. В случае возникновения необходимости получения персональных данных субъекта у третьей стороны следует известить об этом объект ПДн заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных;

- запрещается получать, обрабатывать и вносить в ИСПДн не установленные Федеральными законами "О персональных данных" персональные данные о политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах;

- при принятии решений, затрагивающих интересы субъекта ПДн, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

- защита персональных данных от неправомерного их использования или утраты обеспечивается за счет средств оператора в порядке, установленном Федеральными законом "О персональных данных", Трудовым кодексом Российской Федерации и иными нормативными правовыми актами Российской Федерации;

- передача персональных данных субъекта ПДн третьей стороне не допускается без письменного согласия субъекта, за исключением случаев, установленных федеральными законами Российской Федерации;

- обеспечивается конфиденциальность персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

- в случае выявления недостоверных персональных данных или неправомерных действий с ними сотрудников ООО «ГОРЭКОЦЕНТР+», осуществляющих обработку ПДн, при обращении или по запросу субъекта персональных данных, или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных, ООО «ГОРЭКОЦЕНТР+», как оператор ПДн, обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту, с момента такого обращения или получения такого запроса на период проверки;

- в случае подтверждения факта недостоверности персональных данных субъекта персональных данных сотрудники ООО «ГОРЭКОЦЕНТР+», осуществляющие обработку ПДн, на основании документов, представленных субъектом персональных данных, или его законным представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязаны уточнить персональные данные и снять их блокирование;

- в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, допущенные нарушения должны быть устранены. В случае невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, персональные данные должны быть уничтожены. Об устранении допущенных нарушений или об уничтожении персональных данных ООО «ГОРЭКОЦЕНТР+», как оператор ПДн, обязан уведомить субъекта ПДн, или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган;

- хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

**5. Порядок предоставления информации, содержащей персональные данные**

5.1. Предоставление и пользование информацией, содержащей персональные данные субъекта, осуществляется на основании письменного разрешения директора. Передача и предоставление ПДн законным пользователям должна осуществляться способом, не допускающим возможность несанкционированного доступа к ним посторонних лиц.

Передача информации, содержащей персональные данные субъекта ПДн, другим учреждениям и организациям, осуществляется только при наличии правомерных письменных запросов и с письменного разрешения директора в размере, который позволяет не разглашать излишний объем персональных сведений.

При передаче персональных данных субъекта ПДн оператор должен соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья субъекта ПДн, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными субъектов ПДн в порядке, установленном федеральными законами;

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

- не запрашивать информацию о состоянии здоровья субъекта ПДн, являющегося сотрудником ООО «ГОРЭКОЦЕНТР+», за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции;

- передавать персональные данные субъекта ПДн представителю этого субъекта в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

При обращении с запросом о персональных данных сотрудника ООО «ГОРЭКОЦЕНТР+» к работодателю лица, не уполномоченного федеральным законом на получении персональных данных, либо при отсутствии письменного согласия сотрудника на предоставление его персональных данных работодатель обязан отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

**6. Порядок организации ведения и периодической проверки электронного журнала обращений пользователей информационной системы к ПДн**

6.1. Запросы пользователей информационных систем ПДн предприятия на получение персональных данных, включая лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений.

6.2. Содержание электронного журнала обращений периодически, но не реже одного раза в месяц, проверяется администратором информационной безопасности.

**7. Требования к помещениям, в которых располагаются ИСПДн**

7.1. ПДн, обрабатываемые в ИСПДн, являются информационными данными, защищаемыми в соответствии с требованиями, установленными законодательством Российской Федерации.

7.2. В соответствии с требованиями ИБ, архивы ПДн и ИСПДн (как на электронных, бумажных, так и на иных носителях), оборудование, доступ к которому должен быть ограничен в силу его важности для технологического цикла предприятия (помещения серверных, АТС, АРМов АИБ и т.п.), а также обработка ПДн в ИСПДн должны производиться в помещениях, относящихся к категории «помещения ограниченного доступа».

7.3. Обработка ПДн в ИСПДн также должна производиться в помещениях ограниченного доступа.

7.4. Помещения ограниченного доступа должны располагаться в контролируемой зоне.

7.5. Пребывание посторонних лиц в помещениях разрешено только в сопровождении сотрудников, работающих в указанных помещениях, и только с разрешения руководства вышеупомянутых сотрудников.

7.6. Допуск в помещения ограниченного доступа вспомогательного и обслуживающего персонала (уборщиц, электромонтеров, сантехников и т.д.) производится только в случае служебной необходимости.

7.7. В случае, когда помещения ограниченного доступа располагаются на первых и последних этажах здания, их окна должны быть оснащены сигнализацией.

7.8. Двери помещений ограниченного доступа не должны отличаться от дверей других помещений и не должны иметь обозначающих и предупреждающих надписей и табличек.

7.9. Внутренняя планировка и расположение рабочих мест в помещениях ограниченного доступа должны обеспечивать исполнителям работ недоступность и сохранность доверенных им ПДн.

7.10. На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений ограниченного доступа, очередность и порядок спасения документов, материалов и изделий, содержащих ПДн, а также порядок дальнейшего их хранения.

7.11. Помещения ограниченного доступа, предназначенные для размещения архивов, предназначенные для размещения АРМ выработки ключей шифрования и ЭЦП, предназначенные для размещения оборудования, доступ к которому должен быть ограничен, должны отвечать следующим требованиям:

- помещение должно располагаться в контролируемой зоне;

- двери помещения должны иметь надежные запоры, приспособления для опечатывания, либо должны быть оснащены контроллерами, включенными в систему контроля ограничения доступа;

- желательно наличие видеокамеры включенной в систему видеозаписи, контролирующей вход в помещение;

- должны быть задействованы все меры, исключающие неконтролируемое пребывание в помещении любых лиц, включая сотрудников сокращённое наименование, не допущенных к работе с ПДн;

- помещение должно быть оборудовано датчиками пожарной и охранной сигнализации, желательно имеющими отдельные (не связанные с другими помещениями) шлейфы сигнализации, включенные в пульты охранно-пожарной сигнализации;

- помещение должно быть оборудовано средствами пожаротушения, желательно наличие автономной автоматической системы пожаротушения;

- помещение должно быть оборудовано необходимым количеством стеллажей и/или шкафов для хранения архивных носителей;

- микроклимат (температурно-влажностный режим) помещения должен отвечать требованиям по сохранности архивных носителей, а условия хранения должны исключать возможность их повреждения (коробления, пересыхания, изгиба и вредного воздействия пыли, магнитных и электрических полей или ультрафиолета);

- от двери помещения должны быть резервные ключи;

- помещение, предназначенное для хранения резервных копий, не должно совмещаться с помещением, в котором размещается оборудование, создающее и (или) использующее указанные резервные копии.

- размещение в помещении оборудования и вспомогательных технических средств должно отвечать санитарно-гигиеническим нормам, а также требованиям техники безопасности и пожарной безопасности.

7.12. Работник, осуществляющий хранение архивов и/или резервных копий ИСПДн, должен иметь печать для опечатывания дверей и сейфа или металлического хранилища.

7.13. Выполнение требований по обеспечению ИБ на рабочих местах осуществляется работниками, работающими в помещениях ограниченного доступа.

7.14. Ответственность за невыполнение требований по ИБ для помещений ограниченного доступа несут руководители структурных подразделений, работники которых работают в этих помещениях.

**8. Ответственность за нарушение требований, регулирующих получение, обработку и хранение персональных данных сотрудника**

8.1. Лица, виновные в нарушении требований, регулирующих получение, обработку и хранении персональных данных сотрудника несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

8.2. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы:

- руководитель, разрешающий доступ сотрудника к персональным данным несет персональную ответственность за данное разрешение;

- каждый сотрудник несет единоличную ответственность за сохранность носителей персональных данных и соблюдение конфиденциальности информации;

- сотрудник ООО «ГОРЭКОЦЕНТР+», предоставивший работодателю подложные документы или заведомо ложные сведения о себе, либо своевременно не сообщивший об изменениях персональных данных, несет дисциплинарную ответственность, вплоть до увольнения.

8.3. Лица, виновные в нарушении условий использования средств защиты информации или нарушении режима защиты персональных данных, несут ответственность в соответствии с законодательством Российской Федерации.