АКЦИОНЕРНОЕ ОБЩЕСТВО
САМАРСКАЯ РЕГИОНАЛЬНАЯ ЭНЕРГЕТИЧЕСКАЯ КОРПОРАЦИЯ

ПРИКАЗ

«26» 08 2019 г. № 01-056

Об утверждении документов регламентирующих организацию обработки персональных данных

Во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию ответственного лица за обработку персональных данных в АО СамРЭК (Приложение № 1).
2. Утвердить Положение о парольной защите в АО «СамРЭК» (Приложение № 2).
3. Утвердить Положение по обеспечению антивирусной защиты в АО «СамРЭК» (Приложение № 3).
4. Утвердить Положение по обеспечению информационной безопасности при работе в сети Интернет в АО «СамРЭК» (Приложение № 4).
5. Утвердить Положение о порядке работы с материальными носителями персональных данных т в АО СамРЭК» (Приложение № 5).

6. Утвердить Порядок обработки запросов и обращений субъектов персональных данных и запросов уполномоченного органа по защите прав субъектов персональных данных, поступающих в АО «СамРЭК» (Приложение №6).

7. Утвердить Положение о порядке доступа в помещения АО «СамРЭК», в которых ведется обработка персональных данных, и учета таких помещений (Приложение № 7).

8. Утвердить Положение о порядке обработки и обеспечения безопасности персональных данных в АО «СамРЭК» (Приложение № 8).

9. Утвердить Положение о порядке отнесения автоматизированных систем к информационным системам персональных данных и определении уровней защищенности персональных данных при их обработке в информационных системах персональных данных АО «СамРЭК» (Приложение №9).

10. Утвердить Положение о системе видео наблюдения в АО «СамРЭК» (Приложение №10).

11. Утвердить Перечень подразделений и должностей работников, допущенных к работе с персональными данными, обрабатываемыми наблюдения в АО «СамРЭК» (Приложение №11).

12. Утвердить Перечень персональных данных, обрабатываемых в АО «СамРЭК» (Приложение №12).

13. Утвердить Перечень информационных систем персональных данных АО «СамРЭК» (Приложение №13).

14. Начальнику отдела управления персоналом организовать:

- ознакомление работников АО «СамРЭК» с документами, перечисленными в пунктах 2-8 настоящего приказа;

- оформление под роспись обязательств о соблюдении конфиденциальности персональных данных оформленных согласно приложению 2 Положения о прядке обработки и обеспечения безопасности персональных данных в АО

«СамРЭК», работников АО «СамРЭК» допущенных к обработке персональных данных;

- оформление под роспись обязательств работников АО «СамРЭК», которые выполняют функции, связанные с реализацией договора о передаче полномочий единоличного исполнительного органа общества с ограниченной ответственностью «СамРЭК-Эксплуатация» №2018-000222, о соблюдении конфиденциальности персональных данных;

- на постоянной основе ознакомление вновь принимаемых в АО «СамРЭК» работников вышеперечисленных документов под роспись;

- обеспечить хранение листов ознакомления в отделе управления персоналом.

15. Контроль за исполнением приказа оставляю за собой.

Генеральный директор А.В. Гадалин

Исп. .Баряев С.А.. 212-02-76(355)

Приложение 8

УТВЕРЖДЕНО

приказом АО «СамРЭК»

от 26 08 2019 г. № 01-056

Положение о порядке обработки и обеспечения безопасности персональных данных в АО «СамРЭК»

г. Самара

2019 г.

1. Общие положения

1.1. Настоящее Положение о порядке обработки и обеспечении безопасности персональных данных в АО «СамРЭК» (далее – Положение) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Политикой АО «СамРЭК» в области обработки и обеспечения безопасности персональных данных и иными внутренними документами АО «СамРЭК» (далее – Организация).

1.2. Положение устанавливает единый порядок обработки персональных данных (далее также – ПДн) работников Организации и иных субъектов персональных данных, ПДн которых подлежат обработке в Организации, с целью обеспечения защиты прав субъектов персональных данных на неприкосновенность частной жизни, личную и семейную тайну, а также определяет случаи ответственности работников Организации имеющих доступ к ПДн, за невыполнение требований Положения и иных норм, регулирующих обработку и защиту ПДн субъектов персональных данных Организации.

1.3. В части не урегулированной Положением обработка ПДн работниками Организации осуществляется в соответствии с законодательством Российской Федерации.

1.4. Все работники Организации, которые участвуют в обработке ПДн, должны быть ознакомлены с Положением под роспись.

2. Основные понятия

2.1. В Положении используются следующие основные понятия:

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

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

Обработка персональных данных — 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.

Автоматизированная обработка персональных данных — обработка ПДн с помощью средств вычислительной техники.

Обработка персональных данных без использования средств автоматизации (неавтоматизированная) — обработка ПДн, содержащихся в информационной системе ПДн либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека.

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

Предоставление персональных данных — действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

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

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

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

Использование персональных данных — действия (операции) с ПДн, совершаемые работником Организации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн либо иным образом затрагивающих его права и законные интересы или права и законные интересы других лиц.

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

Общедоступные персональные данные — ПДн, доступ к которым неограниченному кругу лиц предоставлен субъектом ПДн либо по его просьбе, либо с согласия субъекта ПДн или ПДн, на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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

Ресурс персональных данных — совокупность ПДн, обрабатываемых в Организации с использованием или без использования средств автоматизации, в том числе ИСПДн, объединенных общими целями обработки.

Пользователь персональных данных — работник Организации, участвующий в процессе обработки персональных данных или использующий результаты такой обработки.

Конфиденциальность персональных данных — обязательное для соблюдения Организацией или иным получившим от него доступ к ПДн субъекта персональных данных лицом требование не раскрывать третьим лицам и не допускать их распространения при отсутствии согласия субъекта ПДн или иного законного основания.

Целостность персональных данных — способность средства вычислительной техники или информационной системы Организации обеспечивать неизменность ПДн в условиях случайного и (или) преднамеренного их искажения (разрушения).

Доступность персональных данных — возможность беспрепятственного получения санкционированного доступа к ПДн работниками Организации, имеющими право на такой доступ.

Безопасность персональных данных — состояние защищенности персональных данных от неправомерных действий, характеризуемое способностью работников, технических средств и информационных систем Организации обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке, независимо от формы их представления.

Информация — сведения (сообщения, данные), которыми располагает Организация, независимо от формы их представления.

Документированная информация — зафиксированная работником Организации на материальном носителе информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Несанкционированный доступ (несанкционированные действия) — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, реализованных в информационных системах персональных данных Организации.

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Программное обеспечение - комплекс компьютерных программ, обеспечивающий обработку или передачу данных.

Событие информационной безопасности - идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

Машинный носитель персональных данных – съемное или несъемное средство для записи, обработки (хранения) и считывания персональных данных.

Съемный машинный носитель персональных данных – машинный носитель персональных данных, предназначенный для автономного хранения и передачи персональных данных.

3. Принципы и правила обработки персональных данных

3.1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» Организация является оператором ПДн.

3.2. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» обработка ПДн в Организации осуществляется в соответствии со следующими принципами:

- Законности и справедливости обработки ПДн.
- Ограничения обработки ПДн достижением конкретных, заранее определенных и законных целей.
- Недопущения обработки ПДн, несовместимой с целями их сбора.
- Недопущения объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.
- Обработки только тех ПДн, которые отвечают целям их обработки.
- Соответствия содержания и объема обрабатываемых ПДн заявленным целям их обработки.
- Исключения избыточности обрабатываемых ПДн по отношению к заявленным целям их обработки.
- Точности, достаточности и актуальности при обработке ПДн по отношению к целям обработки ПДн.
- Хранения ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.
- Недопущения использования ПДн в целях причинения имущественного и (или) морального вреда субъектам ПДн, затруднения реализации их прав и законных интересов.

3.3. Состав ПДн, а также цели, правовые основания и сроки обработки ПДн Организации содержатся в Перечне персональных данных, обрабатываемых в АО «СамРЭК», утверждаемом Генеральным директором Организации.

3.4. В отношении работников Организации Положение применяется с учетом Положения о работе с персональными данными работников.

3.5. В Организации не осуществляется обработка ПДн, касающихся расовой, национальной принадлежности, политических взглядов, философских и религиозных убеждений, интимной жизни.

3.6. Обработка ПДн, касающихся состояния здоровья работников Организации, допускается исключительно в случаях, предусмотренных трудовым законодательством, включая законодательство об охране труда, и законодательством о социальной защите инвалидов. Обработка таких данных

производится без использования средств автоматизации. Обработка ПДн, касающихся состояния здоровья остальных категорий субъектов ПДн, в Организации не осуществляется.

3.7. В случаях обезличивания Организацией ПДн режим их конфиденциальности снимается.

3.8. В Организации не осуществляется принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

3.9. В Организации не осуществляется трансграничная передача ПДн.

3.10. Организация не создает и не публикует общедоступные источники ПДн, не размещает ПДн субъекта персональных данных в общедоступных источниках без его предварительного согласия.

3.11. Организация вправе поручить обработку ПДн третьему лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. При этом Организация в договоре обязывает лицо, осуществляющее обработку ПДн по поручению, соблюдать конфиденциальность обрабатываемых ПДн, соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3.12. Организация может предоставлять ПДн субъектов персональных данных третьим лицам на основании заключаемых с ними договоров или государственным и муниципальным органам в соответствии с требованиями законодательства Российской Федерации. Передача ПДн осуществляется с согласия субъекта ПДн, за исключением случаев, когда для передачи ПДн имеются иные правовые основания, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3.13. Организация обязуется и требует от иных лиц, получивших доступ к ПДн, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

3.14. Направление в уполномоченный орган по защите прав субъектов ПДн уведомлений об обработке персональных данных осуществляется Организацией в порядке и по основаниям, предусмотренных разделом 12 Положения.

4. Порядок предоставления доступа работникам к персональным данным субъектов персональных данных

4.1. Доступ к ПДн субъектов, обрабатываемым в Организации, имеют работники, которым ПДн необходимы в связи с исполнением ими трудовых (функциональных) обязанностей, в том числе в соответствии с Договором о передаче полномочий единоличного исполнительного органа общества с ограниченной ответственностью «СамРЭК-Эксплуатация» №2018-000222.

Перечень работников Организации, имеющих доступ к ПДн, содержится в Перечне подразделений и лиц, допущенных к работе с персональными данными в АО «СамРЭК», при этом работники имеют право получать и обрабатывать только те ПДн субъекта, которые необходимы им для выполнения их трудовых функций.

4.2. Предоставление работнику Организации доступа к ПДн возможно только при одновременном соблюдении следующих предварительных условий:

- ознакомление работника с Положением и иными локальными нормативными и организационно-распорядительными актами (положения, инструкции, приказы, распоряжения, и т.п.), регулирующими обработку и защиту ПДн в Организации;

- истребование у работника подписанного им письменного обязательства о соблюдении конфиденциальности персональных данных, подготовленного по форме, установленной в приложении 2 к Положению.

4.3. За выполнение перечисленных в пункте 4.2 Положения действий ответственность несет начальник отдела управления персоналом Организации.

4.4. Предоставление работникам Организации доступа к ПДн субъектов осуществляется работниками отдела информационных технологий Организации только при наличии работника в перечне подразделений и лиц, допущенных к работе с персональными данными.

4.5. Контроль за предоставлением минимально необходимых полномочий пользователей по доступу к ПДн и реализацией правил разграничения доступа к ПДн осуществляется работниками отдела информационных технологий Организации.

5. Сбор персональных данных

5.1. Все ПДн о субъекте персональных данных Организация вправе получить непосредственно у субъекта персональных данных.

5.1.1. Если предоставление ПДн является обязательным в соответствии с федеральным законом, Организация обязана разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

5.1.2. В случаях, когда Организация может получить необходимые ПДн субъекта только у третьей стороны, Организация должен уведомить субъекта об обработке его ПДн (за исключением случаев, предусмотренных частью 4 статьи 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных») и при необходимости получить от него письменное согласие по форме, установленной в Организации для оформления согласия соответствующей категории субъектов ПДн.

5.2. Организация вправе проверять достоверность сведений, предоставленных субъектом ПДн, сверяя данные, предоставленные субъектом, с имеющимися у Организации документами, а также по общедоступным источникам информации (включая сведения, содержащиеся в информационно-телекоммуникационной сети «Интернет»).

5.3. В Организации осуществляется сбор согласий на обработку ПДн от следующих категорий субъектов ПДн:

- работников;

- клиентов, и др. (физических лиц, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, индивидуальных предпринимателей);

- членов коллегиальных органов управления, исполнительных органов, главных бухгалтеров и лиц, которым предоставлено право распоряжения денежными средствами, являющихся стороной договоров гражданско-правового характера, заключенных с Организацией.

5.4. Согласие может быть частью договора, заключаемого с субъектом ПДн (в том числе в форме договора присоединения), или оформляться в виде отдельного документа. Согласие на обработку Организацией и иными привлеченными Организацией лицами персональных данных в целях предоставления субъекту ПДн информации о рекламных акциях, маркетинговых исследованиях может быть оформлено отдельным документом и в том случае, когда согласие на обработку ПДн в иных целях включено в текст договора, заключенного с субъектом ПДн.

5.5. Согласие истребуется до или в момент получения ПДн субъекта персональных данных.

5.6. Ответственность за сбор и хранение согласий возлагается на работников подразделений Организациеи, осуществляющих сбор ПДн субъектов персональных данных. Хранение согласий субъектов персональных данных осуществляется в бумажном виде в папках с их делами.

5.9. Порядок отзыва согласия субъекта персональных данных на обработку ПДн:

- Если право или обязанность обработки ПДн субъекта персональных данных Организации установлена законом, то субъект персональных данных обязан не препятствовать реализации Организацией этого права или исполнению этой обязанности.

- В случае отзыва субъектом ПДн согласия на обработку его ПДн работники Организации действуют согласно Регламенту обработки запросов и обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов персональных данных, утвержденному в Организации.

6. Запись, систематизация и накопление персональных данных

6.1. Организация осуществляет запись, систематизацию и накопление полученных ПДн в базах данных и иных электронных хранилищах данных с использованием АС и ПО.

6.2. В случаях, предусмотренных Положением и (или) иными локальными нормативными и организационно-распорядительными актами, регулирующими обработку и защиту ПДн в Организации, в Организации осуществляется накопление ПДн на бумажных носителях. Документы, в зависимости от

содержащихся в них ПДн и целей обработки этих ПДн, должны формироваться работниками Организации в папки, дела и храниться в специально отведенных для этого местах и помещениях, определенных в Перечне помещений, в которых ведется обработка персональных данных, и Перечне мест хранения материальных носителей персональных данных.

7. Хранение персональных данных

7.1. Хранение ПДн в Организации осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки и требования нормативных правовых актов, устанавливающих сроки хранения документов, после чего данные могут быть обезличены (при необходимости).

7.2. Работники Организации, имеющие доступ к ПДн субъектов персональных данных в связи с исполнением трудовых обязанностей, обязаны обеспечивать хранение информации, содержащей ПДн субъектов персональных данных, исключающее неправомерный или случайный доступ к ним.

7.2.1. В случае необходимости работник обязан передать документы и иные носители, содержащие ПДн субъектов персональных данных, работнику, на которого организационно-распорядительным актом (приказом, распоряжением) или должностной инструкцией возложено исполнение его трудовых обязанностей.

7.2.2. В случае увольнении работника, имеющего доступ к ПДн субъектов персональных данных, документы и иные носители, содержащие ПДн субъектов персональных данных, передаются другому работнику, имеющему доступ к ПДн субъектов персональных данных, по указанию руководителя структурного подразделения.

7.3. Помещения, в которых разрешается хранение ПДн, определены в Положении о порядке доступа в помещения АО «СамРЭК», в которых ведется обработка персональных данных, и учета таких помещений.

7.4. Места хранения, а также порядок хранения материальных носителей персональных данных определены в Положении о порядке работы с материальными носителями персональных данных в АО «СамРЭК».

7.5. В Организации ведется учет ИСПДн Организации, ресурсов ПДн и количества субъектов ПДн, в т.ч. не являющихся работниками Организации, для каждого ресурса ПДн.

7.5.1. Перечень ИСПДн Организации с указанием входящих в их состав программного обеспечения обработки ПДн и процессов обработки ПДн содержится в Перечне информационных систем персональных данных в АО «СамРЭК».

7.5.2. Порядок выделения в Организации новой ИСПДн определен в Положении о порядке отнесения автоматизированных систем АО «СамРЭК» к информационным системам персональных данных и определении уровней защищенности персональных данных при их обработке в информационных системах персональных данных.

7.5.3. Учет ресурсов ПДн и количества субъектов ПДн для каждого ресурса ПДн ведется работником, ответственным за организацию обработки ПДн в Организации, в журнале, форма, которого предусмотрена приложением 1 к Положению.

7.5.4. Работник, ответственный за организацию обработки ПДн в Организации, контролирует актуальность учетных данных и вносит изменения в журнал, указанный в подпункте 7.5.3 Положения, в случае обнаружения существенных изменений в перечне ресурсов ПДн или количестве субъектов ПДн.

8. Использование, извлечение и уточнение персональных данных

8.1. В Организации ПДн используются исключительно для достижения целей, предусмотренных Политикой АО «СамРЭК» в области обработки и обеспечения безопасности персональных данных.

8.2. При использовании ПДн допускается:

- извлечение ПДн из баз данных или иных электронных хранилищ данных;
- формирование документов (как в электронном виде, так и на бумажных носителях), содержащих ПДн, в случаях, предусмотренных технологическими процессами обработки ПДн;
- передача таких документов как внутри Организации между работниками, в том числе различных структурных подразделений, так и третьим лицам.

8.3. Организация обязана уточнять обрабатываемые ПДн и вносить в них необходимые изменения (при выявлении неполных или неточных ПДн субъекта персональных данных) в следующих случаях:

- по требованию субъекта ПДн согласно Порядка обработки запросов и обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов персональных данных;
- по требованию уполномоченного органа по защите прав субъектов ПДн согласно Порядка обработки запросов и обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов персональных данных;
- по результатам внутренних контрольных мероприятий.

8.4. Организация обязана уведомить субъекта ПДн или его представителя о внесенных изменениях и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта персональных данных были переданы.

8.5. Лицом, ответственным за организацию и контроль своевременного внесения изменений в ПДн субъектов персональных данных и направления уведомлений субъектам персональных данных, их представителям и третьим лицам, является работник, ответственный за организацию обработки ПДн в Организации.

8.6. Случаи уведомления, а также порядок направления уведомлений субъектам ПДн определены в Порядке обработки запросов и обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов персональных данных.

9. Передача персональных данных

9.1. Передача ПДн может осуществляться посредством использования корпоративной сети Организации (размещения ПДн в сетевых папках, передачи по электронной почте и т.д.), а также с использованием материальных носителей ПДн (бумажных или съемных машинных).

9.2. Передачу ПДн с использованием съемных машинных носителей (магнитных дисков, флеш-дисков, оптических дисков (CD-RW, CD-ROM, ROM DVD, DVD-RW) и других устройств хранения данных) разрешается осуществлять только в случае невозможности использования корпоративной сети.

9.3. Порядок передачи ПДн с использованием материальных носителей (в том числе третьим лицам) устанавливается Положением о порядке работы с материальными носителями персональных данных в АО «СамРЭК».

9.4. При необходимости передачи ПДн другим работникам Организации для исполнения ими своих трудовых обязанностей, допускается осуществлять передачу только работникам, имеющим доступ к ПДн субъектов персональных данных согласно Перечню подразделений и лиц, допущенных к работе с ПДн.

9.5. Предоставление Организацией доступа к ПДн субъекта персональных данных третьим лицам осуществляется при соблюдении следующих условий:

9.5.1. Передача ПДн, в том числе поручение Организацией обработки ПДн третьим лицам осуществляется с согласия субъекта ПДн или без такового согласия при наличии правовых оснований, предусмотренных статьей 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и иных правовых актов.

9.5.2. В том случае, если Организация поручает обработку ПДн третьему лицу на основании договора, в условиях такого договора определяется обязанность лица, осуществляющего обработку ПДн по поручению Организации, по соблюдению конфиденциальности ПДн и обеспечению безопасности ПДн.

9.6. Предоставление ПДн субъекта персональных данных государственным органам и органам местного самоуправления производится в соответствии с требованиями действующего законодательства Российской Федерации и Положением.

9.7. Ответственность за соблюдение порядка предоставления ПДн субъекта персональных данных третьим лицам несет работник Организации, а также руководитель структурного подразделения, осуществляющего передачу ПДн субъекта персональных данных третьему лицу.

10. Блокирование персональных данных

10.1. Организация блокирует обрабатываемые ПДн при выявлении недостоверности обрабатываемых ПДн или неправомерных действий в отношении субъекта персональных данных в следующих случаях:

- по требованию субъекта ПДн согласно Порядка обработки запросов и обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов персональных данных;

- по требованию уполномоченного органа по защите прав субъектов ПДн согласно Порядка обработки запросов и обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов персональных данных;

- по результатам внутренних контрольных мероприятий.

11. Удаление, уничтожение и обезличивание персональных данных

11.1. Организация уничтожает ПДн (удаляет их из автоматизированных систем обработки ПДн, баз данных и иных электронных хранилищ данных, а также уничтожает бумажные носители, содержащие ПДн) по достижении целей обработки ПДн или утраты необходимости в их достижении (допускается также обезличивание ПДн, в результате которого становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту).

11.2. Организация уничтожает ПДн также в случаях:

- получения соответствующего запроса от субъекта ПДн, при условии, что данный запрос не противоречит требованиям законодательства Российской Федерации;

- отзыва согласия субъекта персональных данных на обработку его ПДн (если отзыв согласия влечет за собой уничтожение ПДн);

- получения соответствующего предписания от уполномоченного органа по защите прав субъектов ПДн.

11.3. Уничтожение, обезличивание либо блокирование ПДн в перечисленных в пунктах 11.1-11.2 Положения случаях выполняется согласно Порядка обработки запросов и обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов персональных данных.

11.4. В случае достижения цели обработки ПДн Организация обязана прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) в срок, не превышающий тридцати календарных 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 Организацией и субъектом ПДн либо, если Организация не вправе осуществлять обработку ПДн без согласия субъекта ПДн, по основаниям, предусмотренным федеральными законами. В случае отсутствия возможности уничтожения ПДн в указанный срок, Организация обеспечивает блокирование таких ПДн и обеспечивает их уничтожение в срок не более шести месяцев, если иной срок не установлен федеральными законами.

11.5. Одной из целей обработки ПДн является исполнение требований законодательства Российской Федерации, определяющих сроки хранения документов. Сроки хранения документов исчисляются с 1 января года, следующего за годом окончания их в делопроизводстве. Таким образом, достижением цели обработки ПДн в таком случае будет являться истечение срока хранения, предусмотренного законодательством Российской Федерации или договором или иным соглашением, заключенным с Организацией, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Организацией и субъектом ПДн.

11.6. Удаление, уничтожение или обезличивание ПДн, хранящихся на материальных носителях ПДн, а также уничтожение самих материальных носителей ПДн осуществляются в соответствии с Положением о порядке работы с материальными носителями персональных данных в АО «СамРЭК».

11.7. Ответственность за организацию и контроль прекращения обработки ПДн и их уничтожение по достижении целей обработки несет работник, ответственный за организацию обработки ПДн в Организации. Для выделения информации к уничтожению, а также уничтожения Организацией могут привлекаться сторонние организации, оказывающие соответствующие услуги.

12. Взаимодействие Организации с субъектами персональных данных и органами власти

12.1. Порядок взаимодействия Организации с субъектами ПДн или их законными представителями установлен Регламентом обработки запросов и обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов персональных данных.

12.2. Уполномоченным органом по защите прав субъектов ПДн является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) (далее – Роскомнадзор). Роскомнадзор, в частности, имеет право:

- - осуществлять проверку сведений, содержащихся в уведомлениях об обработке ПДн, и привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

- обращаться к Организации с требованиями по уточнению, блокированию или уничтожению недостоверных или полученных незаконным путем ПДн;

- принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки ПДн, осуществляемой Организацией с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- направлять в ФСБ России и ФСТЭК России сведения о мерах по обеспечению безопасности ПДн, указанных в уведомлениях об обработке ПДн;

- направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн, в соответствии с подведомственностью;

- привлекать к административной ответственности работников Организации, виновных в нарушении требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

12.3. Взаимодействие Организации с Роскомнадзором осуществляется в порядке, предусмотренном приказом Минкомсвязи России от 14.11.2011 № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки ПДн требованиям законодательства Российской Федерации в области ПДн».

12.4. Оценка законности и мотивированности запросов Роскомнадзора о предоставлении информации о процессах обработки ПДн (в т.ч. о предоставлении ПДн), взаимодействие в рамках проведения плановых и внеплановых проверок осуществляется работником, ответственным за организацию обработки ПДн в Организации.

12.5. Запросы субъекта персональных данных, его законного представителя или уполномоченного органа государственной власти по защите прав субъектов ПДн регистрируются в соответствии с Порядком обработки запросов и обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов персональных данных работником, ответственным за организацию обработки ПДн в Организации.

12.6. Порядок направления Организацией уведомления в Роскомнадзор об осуществлении обработки ПДн (далее – Уведомление).

12.6.1. Уведомление направляется в Роскомнадзор согласно статье 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в письменном виде за подписью генерального директора Организации или иного должностного лица, исполняющего его обязанности.

12.6.2. Уведомление должно содержать следующие сведения: наименование и адрес Организации; цель обработки ПДн; категории обрабатываемых ПДн; категории субъектов, ПДн которых обрабатываются; правовое основание обработки ПДн; перечень действий с ПДн, общее описание способов обработки ПДн; описание выполняемых Организацией мер, направленных на обеспечение выполнения Организацией обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»; описание выполняемых Организацией мер по обеспечению безопасности ПДн при их обработке, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств ; фамилия, имя, отчество лица, ответственного за организацию обработки ПДн в Организации, номера его контактного телефона,

почтовый адрес и адрес электронной почты; дата начала обработки ПДн; срок или условие прекращения обработки ПДн; сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки; сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации; сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации, .

12.6.3. В случае изменения указанных в подпункте 12.6.2 Положения сведений Организация обязана уведомить Роскомнадзор в течение десяти рабочих дней с даты возникновения таких изменений.

12.6.4. Ответственность за подачу Уведомления и контроль необходимости направления в Роскомнадзор информационных писем в случаях, предусмотренных пунктом 12.6.3 Положения, несет работник, ответственный за организацию обработки ПДн в Организации.

13. Особенности неавтоматизированной обработки персональных данных

13.1. Обработка ПДн без использования средств автоматизации в Организации осуществляется в соответствии с общими правилами, установленными в разделах 3 – 12 Положения. Дополнительно при неавтоматизированной обработке ПДн должны соблюдаться перечисленные в настоящем разделе требования, основанные на соответствующих положениях Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации».

13.2. При разработке и использовании в Организации стандартных форм документов (в том числе, в виде реестров, журналов, книг), характер информации в которых предполагает или допускает включение в них ПДн, должны выполняться следующие условия:

- форма содержит сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, наименование и адрес Организации, общее описание используемых в Организации способов обработки ПДн, а также поля для указания фамилии, имени, отчества и адреса субъекта ПДн, источников получения ПДн, срока обработки ПДн, перечня действий с ПДн, которые будут совершаться в процессе их обработки;

- форма содержит поле, в котором субъект ПДн может поставить отметку (подпись) о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации (если предоставление Организации заполненной формы предполагает необходимость получения Организации письменного согласия субъекта персональных данных на обработку ПДн);

- содержащиеся в форме ПДн нескольких субъектов персональных данных структурированы способом, исключающим возможность ознакомления субъектов ПДн с персональными данными иных лиц;

- форма не предусматривает объединение полей, предназначенных для внесения ПДн, цели обработки которых Организацией заведомо не совместимы.

13.3. Порядок обработки ПДн на материальных носителях ПДн без использования средств автоматизации предусмотрен Положением о порядке работы с материальными носителями персональных данных в АО «СамРЭК».

14. Общие положения об обеспечении безопасности персональных данных

14.1. Меры по обеспечению безопасности ПДн при их обработке устанавливаются Организацией в соответствии со следующими нормативными правовыми актами:

- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах персональных данных»;
- 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».

14.2. Требования к обеспечению безопасности ПДн реализуются в Организации комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации. Реализация требований к обеспечению безопасности ПДн осуществляется отделом информационных технологий.

14.3. Защиту ПДн в структурных подразделениях Организации, работники которых имеют доступ к ПДн, организуют руководители указанных подразделений в соответствии с требованиями Положения.

14.4. Работником, ответственным за организацию обработки ПДн в Организации ведется учет ресурсов ПДн и ИСПДн. Ресурсы, подлежащие защите, включаются в Журнал учета ресурсов персональных данных и количества субъектов персональных данных для каждого ресурса и в Перечень информационных систем персональных данных АО «СамРЭК». Защите, в частности, подлежат:

- ПДн, содержащиеся в автоматизированных системах обработки ПДн, базах данных и других электронных хранилищах информации;
- ПДн, содержащиеся на бумажных носителях ПДн;
- ПДн, содержащиеся на машинных носителях ПДн;
- средства вычислительной техники, с помощью которых осуществляется обработка ПДн;
- ПДн, передаваемые по каналам связи.

15. Меры по обеспечению безопасности персональных данных

15.1. Процедура создания, изменения, удаления учетных записей пользователей, порядок хранения, использования и изменения паролей пользователей для аутентификации и действий в случае компрометации паролей, а также порядок предоставления прав доступа определяются во внутренних нормативных документах Организации по обеспечению информационной безопасности.

15.2. Порядок хранения персональных аппаратных средств аутентификации регламентирован Положением об обеспечении защиты информации с помощью средств криптографической защиты информации в АО «СамРЭК».

15.3. Порядок записи ПДн на машинные носители ПДн, хранения, учета и уничтожения машинных носителей ПДн, передачи их между работниками Организации и третьим лицам, а также контроль перечисленных процедур определены Положением о порядке работы с материальными носителями персональных данных в АО «СамРЭК».

15.4. Порядок регистрации событий безопасности:

- вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (останова) операционной системы;
- подключение съемных машинных носителей информации к ИСПДн и последующий вывод информации на носители информации;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой ПДн;
- попытки доступа программных средств к определяемым Организацией защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей);
- попытки удаленного доступа.

15.5. Требования к антивирусной защите информации, порядок действий при обнаружении вирусных заражений, а также ответственность работников Организации за выполнение установленного порядка обеспечения антивирусной защиты в Организации определены в Положении по обеспечению антивирусной защиты в АО «СамРЭК».

15.6. Контроль обновления антивирусных баз и программного обеспечения средств антивирусной защиты осуществляется работниками отдела информационных технологий в соответствии с выходом обновлений от производителей средств защиты информации.

15.7. Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации, осуществляется работниками отдела информационных технологий в соответствии с выходом соответствующих обновлений от производителей программного обеспечения и средств защиты информации.

15.8. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется работниками отдела информационных технологий в отношении

администрируемых ими программного обеспечения и средств защиты информации на постоянной основе.

15.9 Контроль состава технических средств, программного обеспечения и средств защиты информации, установленных на рабочих станциях работников Организации, контроль заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИСПДн осуществляется работниками отдела информационных технологий ежеквартально.

15.10. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование осуществляется работниками отдела информационных технологий на постоянной основе.

15.11. Процедуры идентификации и аутентификации субъектов и объектов доступа, управления доступом субъектов к объектам доступа, регистрации событий безопасности и антивирусной защиты в виртуальной инфраструктуре аналогичны описанным в документах, перечисленных в пп. 15.1, 15.3 и 15.5 Положения.

15.12. Порядок доступа в помещения Организации, в которых установлены технические средства обработки ПДн, определен в Положении о порядке доступа в помещения, в которых ведется обработка персональных данных, и учета таких помещений.

15.13. Порядок выявления несанкционированного доступа к ПДн:

15.13.1 К попыткам получения несанкционированного доступа к ПДн относятся:

- сеансы работы в ИСПДн незарегистрированных пользователей;
- сеансы работы пользователей ПДн с нарушением установленного времени доступа;
- сеансы работы пользователей ПДн, срок действия полномочий по обработке персональных данных субъектов ПДн которых истек, либо в состав полномочий которых не входят выявленные действия с ПДн;
- действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой выгоды, методом подбора пароля или иными методами без ведома владельца учетной записи(вследствие случайного разглашения пароля и т.п.);
- действия, направленные на получение несанкционированного доступа к средству вычислительной техники, на котором ведется обработка ПДн;
- несанкционированное внесение изменений в параметры конфигурации программных или аппаратных средств обработки или защиты информации, входящих в состав ИСПДн.

15.13.2. Выявление событий, перечисленных в подпункте 15.13.1 Положения, осуществляется на основании регулярного анализа работниками отдела информационных технологий информации о событиях безопасности, регистрируемой автоматизированными системами, программным обеспечением и средствами защиты информации, используемыми в ИСПДн.

15.13.3. При обнаружении нарушений в ходе проведения анализа, предусмотренного подпунктом 15.13.2 Положения, событие оформляется как инцидент информационной.

15.14. Порядок контроля соответствия принятого порядка обеспечения безопасности ПДн.

15.14.1. Контроль соответствия порядка обеспечения безопасности ПДн, установленного Положением и иными внутренними документами Организации в области защиты ПДн осуществляется работниками, ответственными за обеспечение безопасности ПДн, ежегодно.

15.14.2. Перечень необходимых для осуществления контроля мероприятий определяется работниками, ответственными за обеспечение безопасности ПДн, не позднее 31 декабря текущего года и включается в план мероприятий по обеспечению безопасности ПДн, составляемый на календарный год. План мероприятий по обеспечению безопасности ПДн утверждается Генеральным директором Организации.

15.14.3. Типовой перечень мероприятий, необходимых для осуществления контроля в отдельных подсистемах системы защиты ПДн, приведен в приложении 3 к Положению.

15.14.4. За 3 рабочих дня до начала проведения мероприятий, согласно утвержденному плану, работники, ответственные за обеспечение безопасности ПДн, направляют соответствующее уведомление руководителям структурных подразделений, в которых планируется проведение проверки.

15.14.5. По итогам проведения мероприятий контроля формируется отчет, включающий в себя описательную часть и таблицу соблюдения установленных правил обеспечения безопасности ПДн (форма отчета приведена в приложении 4 к Положению).

15.14.6. При выявлении отклонений от правил обеспечения безопасности ПДн работниками, ответственными за обеспечение безопасности ПДн, оценивается степень критичности выявленных отклонений по следующим критериям:

- отклонение можно исправить в оперативном порядке (например, смена разглашенного пользователем пароля доступа, незначительное изменение правил фильтрации на межсетевом экране и т.п.);

- отклонение невозможно исправить в оперативном порядке и требуется внесение изменений в систему защиты ПДн, компоненты ИСПДн или процессы обработки ПДн.

15.14.7. Отклонения, которые могут быть исправлены в оперативном порядке, устраняются ответственными лицами (администраторами соответствующих систем, работниками отдела информационных технологий).

15.14.8. Вопросы устранения отклонений, которые невозможно исправить в оперативном порядке, выносятся на рассмотрение временной рабочей группы.

15.15. Порядок формирования и работы временной рабочей группы:

15.15.1. Временная рабочая группа создается при необходимости коллегиального принятия решений по вопросам организации работ по обеспечению безопасности ПДн.

15.15.2. Состав временной рабочей группы утверждается Приказом Генерального директора Организации в зависимости от конкретных мероприятий, для выполнения которых она создается.

15.15.3. В состав временной рабочей группы в обязательном порядке включаются работник, ответственный за организацию обработки ПДн в Организации. Дополнительно при необходимости в состав временной рабочей группы могут включаться:

- работники структурных подразделений, отвечающих за автоматизацию технологических процессов;
- руководители структурных подразделений, эксплуатирующих информационные системы;
- работники Правового департамента.

15.15.4. Вопросы, требующие коллегиального принятия решений, рассматриваются на заседаниях временной рабочей группы. Принимаемые рабочей группой решения оформляются протоколом заседания.

16. Заключительные положения

16.1. Права и обязанности работников Организации, допущенных к обработке ПДн субъектов персональных данных, определяются их должностными инструкциями.

16.2. Работники Организации, допустившие разглашение ПДн субъекта персональных данных (передачу их посторонним лицам, в том числе работникам Организации, не имеющим прав доступа к ним), их публичное раскрытие, утрату документов и иных материальных носителей, содержащих ПДн субъекта персональных данных, а также иные нарушения обязанностей по их обработке и защите, установленные Положением, иными внутренними документами Организации в области обработки и защиты ПДн, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 1
к Положению о порядке обработки и обеспечения
безопасности ПДн в АО «СамРЭК»

ЖУРНАЛ [1]
учета ресурсов персональных данных и
количества субъектов персональных данных для каждого ресурса

Дата заполнения журнала: дд.мм.гггг

Наименование ресурса персональных данных	Наименование субъекта персональных данных	Количество субъектов персональных данных
ПДн, обрабатываемые в системе 1С Кадры	Работники	2 тысячи
ПДн, обрабатываемые в 1С Предприятие	Исполнители, подрядчики, агенты и иные лица, являющиеся стороной по договорам гражданско-правового характера, (физические лица, индивидуальные предприниматели) Представители клиентов и контрагентов (юридических лиц, физических лиц, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, индивидуальных предпринимателей), действующие на основании доверенности;	63 тысячи

[1] В Приложении приведен пример заполнения журнала

Приложение 2
к Положению о порядке обработки и обеспечения
безопасности ПДн в АО «СамРЭК»

ОБЯЗАТЕЛЬСТВО[2]
О СОБЛЮДЕНИИ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____,

должность:_____,

структурное подразделение:_____,

обособленное подразделение (при наличии):_____,

обязуюсь:

1. Не разглашать, не раскрывать публично, а также соблюдать установленный действующим законодательством Российской Федерации, Положением о порядке обработки и обеспечения безопасности ПДн в АО «СамРЭК»порядок передачи третьим лицам сведений, составляющих ПДн субъектов персональных данных, которые мне будут доверены или станут известны в рамках выполнения своих должностных обязанностей.

2. Выполнять относящиеся ко мне требования Положения о порядке обработки и обеспечения безопасности ПДн в АО «СамРЭК»и других внутренних документов по обеспечению конфиденциальности ПДн субъектов персональных данных и соблюдению правил их обработки.

3. В случае попытки посторонних лиц получить от меня сведения, составляющие ПДн субъектов персональных данных, немедленно сообщить руководителю своего структурного подразделения и ответственному за организацию обработки ПДн.

4. В случае моего увольнения все носители, содержащие ПДн субъектов (документы и копии документов на бумажных носителях, съемных машинных носителях (магнитных дисках, флеш-дисков, оптических дисках (CD-RW, CD-ROM, ROM DVD, DVD-RW) и других устройств хранения данных), видео- и фотоматериалы и пр.), которые находились в моем распоряжении в связи с выполнением мною трудовых обязанностей во время работы в АО «СамРЭК», передать руководителю своего структурного подразделения или другому работнику по указанию руководителя структурного подразделения.

5. Об утрате или недостаче документов или иных носителей, содержащих ПДн субъектов персональных данных (удостоверений, пропусков и т.п.), ключей от хранилищ, сейфов (металлических шкафов) и о других фактах, которые могут привести к разглашению ПДн

[2] Печатается на одном листе бумаги формата А4 (210×297 мм) с двух сторон.

субъектов персональных данных, а также о причинах и условиях возможной утечки сведений немедленно сообщить руководителю своего структурного подразделения.

Я ознакомлен со следующими внутренними документами АО «СамРЭК»:

- Политика АО «СамРЭК»в области обработки и обеспечения безопасности персональных данных;
- Положение о порядке обработки и обеспечения безопасности персональных данных в АО «СамРЭК»;
- Положение о работе с персональными данными работников;
- Положение о порядке доступа в помещения АО «СамРЭК», в которых ведется обработка персональных данных, и учета таких помещений;
- Положение о порядке работы с материальными носителями персональных данных в АО «СамРЭК»;
- Порядок обработки запросов и обращений субъектов персональных данных и запросов уполномоченного органа по защите прав субъектов персональных данных, поступающих в АО «СамРЭК».

Мне известно, что нарушение мною обязанностей по защите ПДн может повлечь дисциплинарную, гражданско-правовую, уголовную и иную ответственность в соответствии с законодательством Российской Федерации.

Подпись _____ (_____)

«___» _____ 20__ г.

Приложение 3
к Положению о порядке обработки и обеспечения
безопасности ПДн в АО «СамРЭК»

ТИПОВОЙ ПЕРЕЧЕНЬ
КОНТРОЛЬНЫХ ПРОВЕРОК ОТДЕЛЬНЫХ ПОДСИСТЕМ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ АО «СамРЭК»

№ п/п	Вид подсистемы защиты	Вид контрольной проверки
1.1	**Подсистема управления доступом**	соответствие установленных прав доступа (в автоматизированных системах обработки ПДн, базах данных и т.п.) трудовым обязанностям пользователя
1.2		соответствие настроек и условий эксплуатации СЗИ требованиям, указанным в эксплуатационной документации
1.3		процесс идентификации, аутентификации и авторизации при входе пользователя в систему (обращении к информационным ресурсам ИСПДн)
1.4		механизмы блокирования доступа средствами защиты от НСД при выполнении устанавливаемого числа неудачных попыток ввода пароля
1.5		система смены пароля принудительным образом (по истечении срока действия пароля)
1.6		выполнение требований по стойкости пароля к попыткам компрометации
2.1	**Подсистема регистрации и учета**	наличие в системных журналах зарегистрированных попыток НСД
2.2		соответствие настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации
2.3		способы защиты системного журнала регистрации от уничтожения или модификации нарушителем
2.4		места хранения носителей ПДн, сейфы и металлические шкафы, надежность их замков
2.5		выполнение установленного порядка учета и хранения носителей ПДн
2.6		фактическое наличие всех носителей ПДн, в том числе учетных журналов, дел, документов (поступивших, изданных, переведенных на выделенное хранение)
2.7		фактическое наличие всех носителей ПДн, переданных на архивное хранение
2.8		номенклатура дел с целью выделения документов, содержащих ПДн, для передачи в архив или на уничтожение
2.9		правильность проставления регистрационных данных носителей, документов, дел и учетных журналов
2.10		правильность проставления в журнале учета носителей ПДн отметок о движении носителей

№ п/п	Вид подсистемы защиты	Вид контрольной проверки
3.1	**Подсистема обеспечения целостности**	соответствие настроек и условий эксплуатации СЗИ требованиям, указанным в эксплуатационной документации
3.2		наличие экземпляров резервных копий ПДн, предусмотренных в соответствии с внутренними документами АО «СамРЭК»
3.3		целостность созданных резервных копий ПДн путем восстановления данных
3.4		функционирование процедур резервного копирования и восстановления (имитация в специально отведенной тестовой зоне выполнения резервного копирования и восстановления данных при аварийном режиме функционирования системы)
4.1	**Подсистема антивирусной защиты**	наличие установленных программных средств антивирусной защиты на рабочих станциях и серверах
4.2		соответствие настроек и условий эксплуатации СЗИ требованиям, указанным в эксплуатационной документации
4.3		процесс своевременного обновления программных средств антивирусной защиты (в т. ч. баз данных вирусных сигнатур) на всех рабочих и серверных станциях
4.4		процесс полного сканирования системы в режиме реального времени антивирусным средством
4.5		процесс автоматической проверки антивирусным средством используемых отчуждаемых носителей
4.6		процесс принудительной проверки используемых отчуждаемых носителей
4.7		процессы защиты от заражения вредоносным ПО (имитация в специально отведенной изолированной тестовой зоне попыток заражения вредоносным ПО серверных и рабочих станций)
4.8		наличие зафиксированных случаев заражения вредоносным ПО в системных журналах и отчетах
5.1	**Подсистема обеспечения безопасного межсетевого взаимодействия**	соответствие настроек и условий эксплуатации СЗИ требованиям, указанным в эксплуатационной документации
5.2		функционирование системы сегментации сети (имитация в специально отведенной тестовой зоне или в нерабочее время попыток проникновения в «закрытый» сегмент сети из «открытого», в том числе с применением специального ПО)

№ п/п	Вид подсистемы защиты	Вид контрольной проверки
5.3		наличие зафиксированных попыток обращения к «закрытым» ресурсам в системных журналах
6.1	**Подсистема анализа защищенности**	выполнение своевременного обновления ПО, используемого для анализа защищенности, в т. ч. баз данных уязвимостей
6.2		соответствие настроек и условий эксплуатации СЗИ требованиям, указанным в эксплуатационной документации
6.3		наличие зафиксированных попыток НСД (имитация попыток преодоления системы защиты в специально отведенной тестовой зоне или в нерабочее время) в системных журналах
7.1	**Подсистема обнаружения и предотвращения вторжений**	настройки системы обнаружения и предотвращения вторжений в соответствии с эксплуатационной и технической документацией к ней
7.2		информация о срабатывании сигналов тревоги
7.3		ложные срабатывания системы
7.4		соблюдение условий использования системы обнаружения и предотвращения вторжений, предусмотренных эксплуатационной и технической документацией
8.1	**Подсистема защиты от утечек по техническим каналам**	установленные на окнах жалюзи, шторы и т. п. в помещениях, где ведется обработка ПДн
8.2		размещение дисплеев рабочих станций, серверов и демонстрационного оборудования (проекторы, телевизоры и т. п.) таким образом, чтобы исключалась возможность просмотра посторонними лицами текстовой и графической информации, содержащей ПДн
9.1	**Подсистема физической защиты**	электронные журналы СКУД на предмет попыток НСД в защищаемые помещения лиц, не имеющих права доступа в данные помещения
9.2		наличие ключей (в том числе и электронных пропусков) от защищаемых помещений, а также проверка сохранности вторых экземпляров ключей от защищаемых помещений
9.3		заявления об утерянных ключах (в том числе и электронных пропусках), по которым можно получить доступ в защищаемые помещения, а также принятых мер (блокирование электронного пропуска, смена замка)

№ п/п	Вид подсистемы защиты	Вид контрольной проверки
9.4		надежность замков, установленных в защищаемых помещениях
10.1	**Подсистема криптографической защиты**	соответствие настроек и условий эксплуатации СКЗИ требованиям, указанным в эксплуатационной документации
10.2		сохранность эксплуатационной и технической документации и ключевых документов на СКЗИ
10.3		журналы учета СКЗИ, эксплуатационная и техническая документации к ним, а также используемые криптографические ключи на правильность их учета и хранения
10.4		функционирование СКЗИ путем имитации процессов шифрования и дешифрования информации

Приложение 4
к Положению о порядке обработки и обеспечения безопасности ПДн в АО «СамРЭК»

ОТЧЕТ[3]
ПО ИТОГАМ ПРОВЕДЕНИЯ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

№ п/п	Дата проведения мероприятия	Проверка	Заключение о степени выполнения установленных правил	Степень выполнения	Степень критичности выявленных отклонений
1	01.01.2019	Соответствие установленных прав доступа (в автоматизированных системах обработки ПДн, базах данных) трудовым обязанностям пользователя ПДн	Установленные правила доступа соответствуют трудовым обязанностям пользователей ПДн	Выполняется полностью	-
2	01.01.2019	Механизмы блокирования доступа средствами защиты от НСД при выполнении устанавливаемого числа неудачных попыток ввода пароля	Блокирование доступа не осуществляется после пяти неудачных попыток ввода пароля	Не выполняется	Возможно устранить в оперативном порядке

[3] В Приложении приведен пример заполнения отчета