


**УТВЕРЖДЕНА**

Генеральным директором АО «ТЭК-Торг»

« 10 » сентября 2018 г.

(Приказ № 50 от 10. 09 2018)

 Д.А. Сытин

## **ПОЛИТИКА**

**в области обработки персональных данных АО «ТЭК-Торг»  
(вторая редакция)**

**Москва, 2018 г.**

## Содержание

1. Общие положения.....	3
2. Область действия .....	3
3. Перечень ответственных лиц.....	4
4. Принципы обработки персональных данных.....	4
5. Меры, направленные на обеспечение выполнения обязанностей при обработке ПДн.....	5
6. Правила обработки персональных данных .....	5
7. Обязанности Общества при обработке персональных данных.....	7
8. Меры по обеспечению безопасности персональных данных при их обработке.....	8
9. Контроль выполнение требований настоящей Политики.....	8
10. Пересмотр настоящей Политики.....	9
11. История изменений.....	9

## 1. Общие положения

1.1. Настоящая Политика определяет принципы и условия обработки персональных данных в АО «ТЭК-Торг» и разработана с учетом требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и нормативных актов уполномоченных органов государственной власти.

1.2. Для целей настоящей Политики используются следующие основные понятия и сокращения:

**Общество** – АО «ТЭК-Торг».

**Закон** – Федеральный закон от 08.07.2006 № 152-ФЗ «О персональных данных».

**ПДн (персональные данные)** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

**Конфиденциальность ПДн** - обязательное для соблюдения Обществом или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

**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.

**Общедоступные ПДн** - ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн, или на которые в соответствии с законодательством Российской Федерации не распространяется требование соблюдения конфиденциальности.

**НСД (несанкционированный доступ)** - доступ, в том числе случайный, к информации или действия с информацией, нарушающие установленные правила предоставления доступа к информации. Область действия

## 2. Область действия

Действие настоящей Политики распространяется на любое действие (операцию) или совокупность действий (операций) с ПДн, совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн. Требования настоящей Политики обязательны к соблюдению всеми работниками Общества, а также лицами, привлеченными Обществом для выполнения работ, оказания услуг на основании гражданско-правовых договоров.

Настоящая Политика должна быть размещена на сайте Обществе ([www.tektorg.ru](http://www.tektorg.ru))

### **3. Перечень ответственных лиц**

Генеральный директор Общества:

- утверждает политику Общества в области обработки ПДн;
- обеспечивает условия для деятельности работников по обработке ПДн в соответствии с требованиями настоящей Политики;
- отвечает за соблюдение требований настоящей Политики работниками Общества.

Лицо, ответственное за обработку ПДн:

- разрабатывает проект политики Общества в области обработки ПДн;
- осуществляет внутренний контроль за соблюдением Обществом и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;
- доводит до сведения работников Общества положения законодательства Российской Федерации в области ПДн, внутренних документов Общества по вопросам обработки ПДн, требований к защите ПДн;
- организует прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

Руководители структурных подразделений:

- отвечают за соблюдение требований настоящей Политики работниками своих подразделений.

Работники Общества:

- отвечают за соблюдение требований настоящей Политики в рамках выполнения своих должностных обязанностей.

### **4. Принципы обработки персональных данных**

4. 1. Обработка ПДн в Обществе осуществляется с учетом следующих принципов:

- законность целей и способов обработки ПДн и добросовестность при обработке ПДн;
- соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Общества по обработке ПДн;
- соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- достоверность ПДн, их достаточность для целей обработки, недопустимость обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимость объединения созданных для несовместимых между собой целей баз данных ИСПДн.

4. 2. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

4. 3. Обработка ПДн осуществляется только с согласия субъекта ПДн, за исключением случаев, предусмотренных в Законе. Согласие на обработку персональных данных должно быть выражено в форме утверждения или в форме четких активных действий субъекта, Общество должно иметь возможность продемонстрировать такое согласие.

4. 4. При обработке ПДн обеспечивается точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки.

4. 5. Обрабатываемые ПДн подлежат уничтожению, либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом в сроки, установленные Законом.

4. 6. Безопасность ПДн достигается путем исключения НСД к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

## **5. Меры, направленные на обеспечение выполнения обязанностей при обработке ПДн**

5. 1. Назначается лицо, ответственное за организацию обработки ПДн;

5. 2. В Обществе издаются документы, определяющие политику в отношении обработки ПДн, внутренние документы по вопросам обработки ПДн, а также, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

5. 3. Применяются правовые, организационные и технические меры по обеспечению безопасности ПДн в соответствии со статьей 19 Закона;

5. 4. Осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн Закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике Общества в отношении обработки ПДн, внутренним документам Общества;

5. 5. Проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Закона, соотношение указанного вреда и принимаемых в Обществе мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом;

5. 6. Работники Общества, непосредственно осуществляющие обработку ПДн, ознакомляются с положениями законодательства Российской Федерации в области ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику Общества в отношении обработки ПДн, внутренними документами Общества по вопросам обработки ПДн, и (или) проходят обучение.

## **6. Правила обработки персональных данных**

6. 1. Обработка ПДн осуществляется с соблюдением принципов и правил, установленных Законом.

6. 2. Обработка ПДн допускается, если:

- осуществляется с согласия субъекта ПДн на обработку его ПДн;
- необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Общество функций, полномочий и обязанностей;

- необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
- необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- необходима для осуществления прав и законных интересов Общества или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания ПДн, за исключением обработки ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;
- осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн, либо по его просьбе;
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

6. 3. Общество может включать ПДн субъектов в общедоступные источники ПДн в случае получения письменного согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.

6. 4. ПДн специальных категорий и биометрические ПДн в Обществе не обрабатываются.

6. 5. Общество не осуществляет трансграничную передачу ПДн.

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

6. 7. При отсутствии необходимости письменного согласия субъекта на обработку его ПДн согласие субъекта может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме.

6. 8. Общество вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. При этом Общество обязывает лицо, осуществляющее обработку ПДн по поручению Общества, соблюдать принципы и правила обработки ПДн, предусмотренные федеральным законом.

6. 9. В случае, если Общество поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Общество. Лицо, осуществляющее обработку ПДн по поручению Общества, несет ответственность перед Обществом.

6. 10. Общество обязуется и обязывает своих работников, а также лиц, привлеченных Обществом к выполнению работ, оказанию услуг на основании гражданско-правовых договоров, получивших доступ к ПДн, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

6. 11. При обработке ПДн в Обществе реализуются следующие процедуры:

- 6.11. 1. направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области ПДн. В этих целях утверждается должностная инструкция работника Общества, ответственного за обработку ПДн, в которой предусматривается осуществление внутреннего контроля за процессом обработки ПДн;
- 6.11. 2. для каждой цели обработки ПДн определяется:
  - перечень обрабатываемых ПДн;
  - категории субъектов ПДн;
  - сроки их обработки и хранения;
  - порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.
- 6.11. 3. категория субъектов ПДн определяется в соответствии с политикой защиты ПДн;
- 6.11. 4. содержание и сроки обработки ПДн должны быть определены в согласии субъекта на обработку ПДн, либо в соответствующих договорах на обработку ПДн.
- 6.11. 5. порядок уничтожения ПДн определен в пункте 7.1. настоящей Политики.

## **7. Обязанности Общества при обработке персональных данных**

7. 1. В соответствии с требованиями Закона Общество обязано:
  - предоставлять субъекту ПДн по его запросу информацию, касающуюся обработки его ПДн, либо на законных основаниях предоставить отказ;
  - по требованию субъекта ПДн уточнять обрабатываемые ПДн, блокировать или удалять, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
  - вести учет обращений субъектов ПДн;
  - уведомлять субъекта ПДн об обработке ПДн в том случае, если ПДн были получены не от субъекта ПДн, за исключением случаев:
    - уведомления субъекта ПДн об осуществлении обработки его ПДн соответствующим оператором,
    - получения ПДн Обществом на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн,
    - обработки общедоступных ПДн или их получения из общедоступного источника,
    - когда предоставление субъекту ПДн сведений, содержащихся в уведомлении об обработке ПДн, нарушает права и законные интересы третьих лиц;
  - в случае достижения цели обработки ПДн незамедлительно прекратить обработку ПДн и уничтожить либо обезличить соответствующие ПДн 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 Обществом и субъектом ПДн либо, если Общество не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Законом или другими федеральными законами;

- в случае отзыва субъектом ПДн согласия на обработку своих ПДн прекратить обработку ПДн и уничтожить либо обезличить ПДн в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Обществом и субъектом ПДн. Об уничтожении ПДн Общество обязано уведомлять субъекта ПДн;
- в случае поступления требования субъекта о прекращении обработки ПДн в целях продвижения товаров, работ, услуг на рынке немедленно прекратить обработку ПДн.

## **8. Меры по обеспечению безопасности персональных данных при их обработке**

8.1. При обработке ПДн Общество принимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

8.2. Обеспечение безопасности ПДн достигается, в частности:

- определением угроз безопасности ПДн при их обработке в ИСПДн;
- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- учетом машинных носителей ПДн;
- обнаружением фактов несанкционированного доступа к ПДн и принятием мер;
- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- обучение работников Общества, участвующих в обработке ПДн, вопросам обеспечения безопасности ПДн.
- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности ИСПДн.

## **9. Контроль выполнения требований настоящей Политики**

9.1. В Обществе проводятся регулярные проверки соблюдения требований Закона.

9.2. Назначается лицо, ответственное за обработку ПДн, в обязанности которого, в том числе, включается осуществление внутреннего контроля за соблюдением Обществом и его



работниками законодательства Российской Федерации в области ПДн, в том числе требований к защите ПДн;

9.3. В Обществе назначается структурное подразделение, отвечающее за защиту ПДн.

#### **10. Пересмотр настоящей Политики**

Положения настоящей Политики подлежат пересмотру в случае изменения требований законодательства Российской Федерации в области обработки персональных данных. Регламентный пересмотр настоящей Политики осуществляется не реже, чем один раз в три года.

#### **11. История изменений**


<b>Версия</b>	<b>Дата изменения</b>	<b>Автор</b>	<b>Описание изменения</b>
1	04.02.2016	Федоров Б.В.	Разработка документа
2	28.08.2018	Федоров Б.В.	Изменение формы собственности, условия согласия

**УТВЕРЖДЕНА**

Генеральным директором АО «ТЭК-Торг»

«10» сентября 2018 г.

(Приказ № 50 от 10 . 09 2018)

 Д.А. Сытин

**Политика**

в области защиты персональных данных в АО «ТЭК-Торг»  
(вторая редакция)

**Москва 2018**

## Содержание

1. Введение.....	3
2. Область действия.....	4
3. Перечень ответственных лиц.....	4
4. Общие положения .....	4
5. Мероприятия по обеспечению безопасности ПДн при их обработке с использованием средств автоматизации .....	5
6. Определение уровня защищенности ИСПДн .....	8
7. Приобретение и разработка ИСПДн.....	8
8. Мероприятия по обеспечению безопасности ПДн при их обработке без использования средств автоматизации .....	9
9. Порядок пересмотра.....	10
10. История изменений.....	10
11. Приложение № 1 АКТ об определении необходимого уровня защищенности информационной системы персональных данных.....	11
12. Приложение № 2 Описание защитных мер информационной системы обработки персональных данных.....	12
13. Приложение № 3 Перечень персональных данных, обрабатываемых в АО «ТЭК-Торг» в ИСПДн.....	17
14. Приложение № 4 Журнал учета носителей персональных данных.....	18

## 1. Введение

1.1. Настоящая Политика является частной политикой информационной безопасности по обеспечению защиты персональных данных, обрабатываемых в АО «ТЭК-Торг».

1.2. Настоящая Политика определяет принципы и условия обеспечения защиты персональных данных в АО «ТЭК-Торг» и разработана с учетом требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и нормативных актов уполномоченных органов государственной власти.

1.3. Для целей настоящей Политики используются следующие основные понятия и сокращения:

**АИС** – автоматизированные информационные системы Общества.

**Акт** – Акт об определении необходимого уровня защищенности информационной системы персональных данных, оформляемый в соответствии с Приложением № 1 к настоящей Политике.

**Аутентификация** — проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

**Закон** – Федеральный закон от 08.07.2006 № 152-ФЗ «О персональных данных».

**ИБ** – информационная безопасность Общества.

**Идентификация** — процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Инцидент** - действительное, предпринимаемое или вероятное нарушение ИБ, которое может быть вызвано либо ошибкой персонала, либо неправильным функционированием технических средств, либо природными факторами (например, пожар или наводнение), либо преднамеренными злоумышленными действиями, приводящими к нарушению конфиденциальности, целостности, доступности, учитываемости или безотказности.

**ИСПДн (информационная система ПДн)** - совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации.

**Общество** – АО «ТЭК-Торг»;

**Конфиденциальность ПДн** - обязательное для соблюдения Компанией или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

**НСД (несанкционированный доступ)** - доступ, в том числе случайный, к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых АИС.

**Модель нарушителя** - предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак на АИС, а также об ограничениях на эти возможности.

**Модель угроз** - перечень возможных угроз.

**Обработка ПДн** - действия (операции) с ПДн, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

**Общедоступные ПДн** - ПДн, к которым доступ неограниченного круга лиц предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**ОИБ** – Отдел информационной безопасности Общества.

**Описание** – «Описание средств защиты информационной системы персональных данных», заполняемое в соответствии с Приложением № 2 к настоящей Политике.

**ПДн (персональные данные)** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

**ПО** – программное обеспечение Общества.

**Постановление** - Постановления Правительства от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

**СКЗИ** – средство криптографической защиты информации.

**Частная модель угроз** – модель угроз для определенной категории защищаемых объектов.

## **2. Область действия**

Действие настоящей Политики распространяется на любые АИС Общества на всех этапах жизненного цикла, в которых совершаются действия (операции) с ПДн, а также на процессы обработки ПДн без использования средств автоматизации, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн. Требования настоящей Политики обязательны к соблюдению всеми работниками Общества, а также лицами, привлеченными Компанией к выполнению работ, оказанию услуг на основании гражданско-правовых договоров.

## **3. Перечень ответственных лиц**

Генеральный директор Общества:

- утверждает политику Общества в области защиты ПДн;
- обеспечивает условия для выполнения работниками Общества требований настоящей Политики;
- отвечает за соблюдение требований настоящей Политики работниками Общества.

Начальник ОИБ:

- разрабатывает проект политики Общества в области защиты ПДн;
- разрабатывает частную модель угроз безопасности ПДн при их обработке с привлечением ресурсов Общества;
- определяет уровень защищенности ИСПДн и обеспечивает соответствие защитных мер и средств установленному уровню защищенности;
- осуществляет внутренний контроль за соблюдением в Обществе требований законодательства Российской Федерации, нормативных актов уполномоченных государственных органов власти, а также внутренних документов Общества к защите ПДн;
- организует повышение осведомленности работников Общества в области защиты ПДн;
- отвечает за адекватность защитных мер актуальным угрозам безопасности ПДн и работоспособность средств защиты.

Руководители структурных подразделений:

- отвечают за соблюдение требований настоящей Политики в рамках своих компетенций.

Работники Общества:

- отвечают за соблюдение требований настоящей Политики при выполнении своих должностных обязанностей.

ОИБ является подразделением Общества, ответственным за обеспечение безопасности ПДн, а также за разработку и проведение мероприятий по обеспечению безопасности ПДн.

#### 4. Общие положения

4.1. Обработка ПДн в Обществе осуществляется с учетом следующих принципов:

- законность целей и способов обработки ПДн и добросовестность при их обработке;
- соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПД, а также полномочиям Общества по обработке ПДн;
- соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- достоверность ПДн, их достаточность для целей обработки, недопустимость обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимость объединения созданных для несовместимых между собой целей баз данных ИСПДн.

4.2. Руководители структурных подразделений Общества составляют список лиц, допущенных к обработке ПДн, который утверждается руководителем Общества.

4.3. Руководители структурных подразделений Общества, занимающиеся обработкой ПДн, составляют перечень ПДн, обрабатываемых в соответствующем подразделении по форме Приложения № 3 к настоящей Политике, и направляют его в ОИБ.

4.4. ОИБ формирует общий Перечень ПДн, обрабатываемых в Обществе, который утверждается руководителем Общества.

4.5. ПДн классифицируются в соответствии со степенью тяжести последствий потери свойств безопасности ПДн для субъекта ПДн, при этом выделяются следующие категории:

- категория С - ПДн, отнесенные в соответствии с Законом к специальным категориям ПДн;
- категория Б - ПДн, отнесенные в соответствии с Законом к биометрическим ПДн;
- категория И - ПДн, которые не могут быть отнесены к специальным категориям ПДн, к биометрическим ПДн, к общедоступным или обезличенным ПДн;
- категория Д - ПДн, отнесенные в соответствии с Законом к общедоступным или обезличенным ПДн;
- категория Р – ПДн работников Общества.

4.6. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, и ПДн подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении в срок, установленный Законом.

4.7. Обработка ПДн осуществляется только с согласия субъекта, за исключением случаев, предусмотренных в Законе.

4.8. Любая ИСПДн должна включать средства защиты информации, обеспечивающие конфиденциальность, целостность и доступность ПДн в соответствии с их категорией. Для категории ПДн-Д условия конфиденциальности не обеспечиваются.

4.9. Безопасность ПДн достигается путем исключения НСД к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

4.10. Безопасность ПДн при их обработке в АИС обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения НСД, программно-технических воздействий на средства обработки ПДн), а также используемые в АИС информационные технологии.

## **5. Мероприятия по обеспечению безопасности ПДн при их обработке с использованием средств автоматизации**

5.1. В целях исполнения требований Закона в Общества проводятся мероприятия по защите ПДн, которые, в том числе, включают определение:

- частной модели угроз безопасности ПДн;
- типа актуальных угроз безопасности ПДн;
- состава, категории и объема обрабатываемых ПДн для каждой ИСПДн;
- уровня защищенности ИСПДн;
- состава необходимых защитных мер и средств для организации безопасной обработки ПДн.

5.2. Для каждой ИСПДн производится анализ возможных угроз и их актуальность с учетом категорий обрабатываемых ПДн, результатом такого анализа является частная модель угроз безопасности ИСПДн, содержащая актуальные для Общества угрозы ИБ, на основе которой вырабатываются требования по обеспечению безопасности ПДн, учитывающие особенности их обработки в Общества. Применяемые меры и средства защиты ПДн учитываются в Описании, а эксплуатационная и техническая документации к ним – в соответствии со сводной номенклатурой дел Общества.

5.3. ИСПДн и средства доступа к ним устанавливаются в помещениях, оборудованных системами контроля и регистрации доступа. Такие помещения в нерабочее время должны ставиться на сигнализацию или опечатываться.

5.4. Обмен ПДн при их обработке в АИС осуществляется по каналам связи, защита которых обеспечивается путем реализации организационных мер и (или) путем применения технических средств.

5.5. При передаче ПДн должны быть соблюдены следующие правила:

- несанкционированный доступ к ПДн в процессе передачи должен быть исключен;
- передача ПДн возможна только в том случае, если обеспечивается конфиденциальность передаваемой информации. Если Общество на основании договора поручает обработку ПДн другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности и безопасности ПДн при их передаче;
- не сообщать ПДн субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника Общества, а также случаях, предусмотренных Трудовым кодексом Российской Федерации и иными федеральными законами;
- не сообщать ПДн субъекта в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих ПДн 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;
- передавать ПДн субъекта представителям субъектов ПД в порядке, установленном законодательством Российской Федерации и ограничивать эту информацию только теми ПДн, которые необходимы для выполнения указанными представителями их функций.

5.6. Для обеспечения безопасности ПДн СКЗИ используются в следующих случаях:

- если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;

- если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

Кроме того, решение о необходимости криптографической защиты ПДн может быть принято Компанией на основании технико-экономического сравнения альтернативных вариантов обеспечения требуемых характеристик безопасности информации, содержащей, в том числе, ПДн.

5.7. К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, относятся:

- передача ПДн по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче ПДн по информационно-телекоммуникационным сетям общего пользования);

- хранение ПДн на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

5.8. Решение о необходимости применения СКЗИ принимается с учетом следующих особенностей:

- криптографическая защита персональных данных может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ;

- СКЗИ штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СКЗИ требований и которые образуют среду функционирования СКЗИ;

- СКЗИ не предназначены для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СКЗИ не предназначены для защиты персональных данных от раскрытия лицами, которым предоставлено право на доступ к этой информации);

- СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ;

- для обеспечения безопасности ПДн при их обработке в ИСПДн должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия;

- СКЗИ являются как средством защиты персональных данных, так и объектом защиты.

5.9. Общество может поручить обработку ПДн третьим лицам (принимающей стороне) на основании заключаемого с этими лицами договором, причем существенным условием договора является обязанность обеспечения третьей стороной конфиденциальности ПДн, целей обработки ПДн и безопасности ПДн при их обработке.

5.10. При обработке ПДн в АИС должно обеспечиваться:

- проведение мероприятий, направленных на предотвращение НСД к ПД и (или) передачи их лицам, не имеющим права доступа к такой информации;

- своевременное обнаружение фактов НСДн к ПДн;

- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;



– возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;

– постоянный контроль за обеспечением уровня защищенности ПДн.

5.11. Установка и ввод в эксплуатацию средств защиты информации осуществляется в соответствии с эксплуатационной и технической документацией.

5.12. Перед вводом в эксплуатацию ИСПД проводится проверка готовности средств защиты ПДн к использованию, в соответствии с пунктом 4. настоящей Политики и инструкцией по эксплуатации этих средств. С учетом результатов проверки делается заключение о возможности их эксплуатации.

5.13. Съёмные носители ПДн учитываются в Журнале учета по форме Приложения №4 к настоящей Политике, который ведется в структурном подразделении Общества, занимающемся формированием таких носителей.

5.14. По достижении цели обработки ПДн на съёмном носителе информация с такого носителя удаляется способом, не позволяющим восстановить удаленную информацию.

5.15. Контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией, осуществляет ОИБ.

5.16. Руководители структурных подразделений Общества организуют обучение подчиненных им работников, использующих средства защиты информации, применяемые в ИСПДн, правилам работы с ними.

5.17. По фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации или другим нарушениям, приводящим к снижению уровня защищенности ПДн, ОИБ по указанию (распоряжению) Генерального директора Общества проводит внутреннее расследование, по итогам которого составляется заключение, а также разрабатываются и принимаются меры по предотвращению возможных опасных последствий подобных нарушений.

5.18. При обнаружении нарушений порядка предоставления ПДн ОИБ незамедлительно приостанавливает предоставление ПДн пользователям АИС до выявления причин нарушений и устранения этих причин.

## **6. Определение уровня защищенности ИСПДн**

6.1. Исходя из актуальных угроз безопасности ПДн, категории ПДн и их объема для каждого ИСПДн определяется необходимый уровень защищенности в соответствии с требованиями Постановления.

6.2. На все действующие и приобретаемые ИСПДн руководитель структурного подразделения Общества, осуществляющего эксплуатацию данной АИС в рамках выполнения функций подразделения, должен предоставить в ОИБ перечень ПДн, обрабатываемых в этой АИС, по форме Приложения № 3 к настоящей Политике и обоснование необходимости обработки ПДн в этой ИСПДн.

6.3. На основании предоставленных данных ОИБ определяет категорию обрабатываемых ПДн.

6.4. Исходя из проектной и эксплуатационной документации и особенностей среды функционирования ИСПДн ОИБ определяет тип актуальных угроз безопасности ПДн для данного ИСПДн.

6.5. На основании информации, определенной в пунктах 6.2. – 4.4. настоящей Политики определяется уровень защищенности ИСПДн, о чем составляется Акт.

6.6. ОИБ заполняет Описание для каждой ИСПДн и анализирует достаточность защитных мер на основании принятой частной модели угроз, после чего проводится

тестирование защитных мер и составляется акт о возможности ввода ИСПДн в эксплуатацию или даются рекомендации по доработке защитных мер.

6.7. При необходимости доработки защитных мер составляется план мероприятий, после реализации которого выполняются действия по пункту 6.6. настоящей Политики.

## **7. Приобретение и разработка ИСПДн**

7.1. При приобретении Компанией новых ИСПДн такие АИС анализируются на соответствие установленным требованиям по защите ПДн, а так же на возможность подключения к ним необходимых средств защиты информации.

7.2. Договор на приобретение новых ИСПДн согласовывается с начальником ОИБ.

7.3. В эксплуатационной документации ИСПДн должны быть отражены вопросы обеспечения безопасности ПДн.

7.4. На этапе согласования проекта договора на приобретение ИСПДн или на этапе проектирования ИСПДн руководитель структурного подразделения Общества, инициирующего закупку или разработку, должен предоставить в ОИБ сведения, перечисленные в пункте 3.2. настоящей Политики.

7.5. Для приобретаемых ИСПДн выполняется пункты 6.6. и 6.7. настоящей Политики.

7.6. Для разрабатываемых ИСПДн ОИБ составляет Описание, на основании которого в технический проект вносятся требования по реализации мер по защите информации.

7.7. Тестирование защитных мер производится на этапе приемо-сдаточных испытаний ИСПДн.

7.8. Работы по обеспечению безопасности ПДн при их обработке в АИС являются обязательной частью работ по созданию АИС.

7.9. Техническое задание, технический проект на разработку новых ИСПДн согласовывается с начальником ОИБ.

7.10. В рабочую группу по разработке новых ИСПДн должен быть включен начальник ОИБ.

## **8. Мероприятия по обеспечению безопасности ПДн при их обработке без использования средств автоматизации**

8.1. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

8.2. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель ПДн.

8.3. Работники Общества, осуществляющие обработку ПДн без использования средств автоматизации (в том числе лица, осуществляющие такую обработку по договору с Компанией), должны быть проинформированы о факте обработки ими ПДн, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также внутренними документами Общества.

8.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), за исключением типовых форм договоров, должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, наименование и адрес Общества, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых в Обществе способов обработки ПДн;

- в типовой форме предусматривается поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн - при необходимости получения такого согласия;

- типовая форма составляется таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

- типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

8.5. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе ПДн, если материальный носитель ПДн не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, принимаются меры по обеспечению раздельной обработки ПДн, в частности:

- при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе ПДн других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель ПДн с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

8.6. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем ПДн, производится способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе ПДн (удаление, вымарывание).

8.7. ПДн (материальные носители), обработка которых осуществляется в различных целях, хранятся раздельно.

8.8. Материальные носители ПДн хранятся в запирающихся на ключ металлических шкафах (сейфах), в помещениях с ограниченным доступом. Помещения, где хранятся ПДн и обрабатываются должны быть оборудованы системой контроля и управления доступом, а в нерабочее время, ставятся на сигнализацию или опечатываются.

8.9. На металлических шкафах (сейфах), в которых хранятся материальные носители ПДн, наносятся сведения, содержащие:

- категорию ПДн;
- список работников Общества, допущенных к работе с этими материальными носителями ПДн.

8.10. На материальный носитель ПДн наносится информация о месте его хранения.

8.11. Уничтожение ПДн в ручном режиме оформляется актом об уничтожении ПДн.

## **9. Пересмотр настоящей Политики**

9.1. Положения настоящей Политики подлежат пересмотру в случаях изменений:

- требований законодательства Российской Федерации в области обработки персональных данных;
- архитектуры программно-аппаратных комплексов Общества;
- бизнес процессов Общества, затрагивающих обработку персональных данных.

9.2. Регламентный пересмотр настоящей Политики производится раз в три года в случае, если она не пересматривалась в соответствии с п. 9.1. настоящего Положения более указанного срока.

#### 10. История изменений

Версия	Дата изменения	Автор	Описание изменения
1	04.02.2016	Федоров Б.В.	Разработка документа
2	28.08.2018	Федоров Б.В.	Новая форма собственности

УТВЕРЖДАЮ  
Генеральный директор АО «ТЭК-Торг»

\_\_\_\_\_ Д.А. Сытин

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**АКТ**  
об определении необходимого уровня защищенности  
информационной системы персональных данных

\_\_\_\_\_ (наименование информационной системы)

На основании изучения и анализа характера персональных данных (далее – ПДн), обрабатываемых в информационной системе \_\_\_\_\_ (наименование) (далее – ИСПДн), а также характеристик самой ИСПДн сделаны следующие выводы:

1. В ИСПДн обрабатываются ПДн категорий \_\_\_\_\_ (Б, С, И, Д, Р, указать нужное) (по определениям «Политики в области защиты персональных данных в АО «ТЭК-Торг».
2. Количество субъектов ПДн, обрабатываемых в ИСПДн, \_\_\_\_\_ (менее ста тысяч или более ста тысяч, указать нужное).
3. Актуальные угрозы безопасности ПДн \_\_\_\_\_ типа (по определениям Постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119).
4. По своей структуре ИСПДн является автономным комплексом аппаратно-программных средств (или комплексом автоматизированных рабочих мест, объединенных в единую информационную систему без использования технологии удаленного доступа/с использованием технологии удаленного доступа – нужное оставить).
5. ИСПДн имеет /не имеет подключение к сетям связи общего доступа (и/или доступ к международным сетям обмена информацией).
6. ИСПДн является однопользовательской/многопользовательской системой.
7. ИСПДн является системой с разграничением/без разграничения прав доступа.
8. Все технические средства ИСПДн находятся в пределах Российской Федерации (или нет – нужное указать).

Исходя из вышеизложенного в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 ИСПДн нуждается в \_\_\_\_\_ уровне защищенности, в связи с чем необходимо внедрить соответствующий набор защитных и/или компенсирующих мер в соответствии с требованиями Приказа ФСТЭК России от 18 февраля 2013 г. N 21.

Технический директор \_\_\_\_\_ 20\_\_ г.  
(ФИО) (Подпись)

Начальник Отдела ИБ \_\_\_\_\_ 20\_\_ г.  
(ФИО) (Подпись)

## Описание защитных мер информационной системы персональных данных автоматизированная система обработки ПДн

Мера защиты	Инструмент защиты	Наличие	Примечания
Идентификация и аутентификация субъектов доступа и объектов доступа	1. Идентификация и аутентификация пользователей, являющихся работниками Общества		
	2. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных		
	3. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов		
	4. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации		
	5. Защита обратной связи при вводе аутентификационной информации		
	6. Идентификация и аутентификация пользователей, не являющихся работниками Общества (внешних пользователей)		
Управление доступом субъектов доступа к объектам доступа	1. Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей		
	2. Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа		
	3. Управление (филترация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы ПДн, а также между информационными системами ПДн		
	4. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы ПДн		
	5. Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы ПДн		
	6. Ограничение неуспешных попыток входа в информационную систему ПДн (доступа к информационной системе)		
	7. Блокирование сеанса доступа в информационную систему ПДн после установленного времени бездействия (неактивности) пользователя или по его запросу		
	8. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		
	9. Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети		
	10. Регламентация и контроль использования в информационной системе ПДн технологий		

Мера защиты	Инструмент защиты		Наличие	Примечания
	беспроводного доступа			
Ограничение программной среды	11. Регламентация и контроль использования в информационной системе мобильных технических средств			
	12. Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)			
	13. Обеспечение доверенной загрузки средств вычислительной техники			
	1. Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			
Защита машинных носителей персональных данных	2. Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов			
	1. Учет машинных носителей персональных данных			
	2. Управление доступом к машинным носителям персональных данных			
	3. Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации			
Регистрация событий безопасности	4. Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания			
	1. Определение событий безопасности, подлежащих регистрации, и сроков их хранения			
	2. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации			
	3. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения			
Антивирусная защита	4. Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти			
	5. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			
	6. Генерирование временных меток и (или) синхронизация системного времени в информационной системе			
	7. Защита информации о событиях безопасности			
Обнаружение вторжений	1. Реализация антивирусной защиты			
	2. Обновление базы данных признаков вредоносных компьютерных программ (вирусов)			
	1. Обнаружение вторжений			
	2. Обновление базы решающих правил			
Контроль (анализ) защищенности персональных данных	1. Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей			
	2. Контроль установок обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации			
	3. Контроль работоспособности, параметров настройки и правильности функционирования			

Мера защиты	Инструмент защиты		Наличие	Примечания
	программного обеспечения и средств защиты информации			
	4. Контроль состава технических средств, программного обеспечения и средств защиты информации			
	5. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			
Обеспечение целостности информационной системы и персональных данных	1. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			
	2. Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций			
	3. Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			
Обеспечение доступности персональных данных	1. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование			
	2. Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			
	3. Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			
	4. Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации			
Защита среды виртуализации	1. Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации			
	2. Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин			
	3. Регистрация событий безопасности в виртуальной инфраструктуре			
	4. Управление (филь-трация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры			
	5. Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			
	6. Контроль целостности виртуальной инфраструктуры и ее конфигураций			
	7. Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			
	8. Реализация и управление антивирусной защитой в виртуальной инфраструктуре			
	9. Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей			
Защита технических средств	1. Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также			



Мера защиты	Инструмент защиты		
	средства обеспечения функционирования	Наличие	Примечания
Защита информационной системы ПДн, ее средств, систем связи и передачи данных	2. Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, включающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены		
	3. Размещение устройств вывода (отображения) информации, включающее ее несанкционированный просмотр		
	1. Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы		
	2. Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи		
	3. Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств		
	4. Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрации событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода		
	5. Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи		
	6. Контроль санкционированной и исключение несанкционированной передачи видеoinформации, в том числе регистрация событий, связанных с передачей видеoinформации, их анализ и реагирование на нарушения, связанные с передачей видеoinформации		
	7. Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов		
	8. Исключение возможности отрицания пользователем факта отправки информации другому пользователю		
	9. Исключение возможности отрицания пользователем факта получения информации от другого пользователя		
	10. Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных		
	11. Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы		
	12. Защита информационной системы от угроз безопасности информации, направленных на отказ в		

Мера защиты	Инструмент защиты	Наличие	Примечания
	обслуживании информационной системы		
	13. Защита периметра (физических и (или) логических границ) информационной системы ПДн при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями		
	14. Прекращение сетевых соединений по их завершении или по истечении заданного в Общества временного интервала неактивности сетевого соединения		
	15. Защита мобильных технических средств, применяемых в информационной системе ПДн		
	16. Защита беспроводных соединений, применяемых в информационной системе		
Выявление инцидентов и реагирование на них	1. Определение лиц, ответственных за выявление инцидентов и реагирование на них		
	2. Обнаружение, идентификация и регистрация инцидентов		
	3. Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе ПДн пользователями и администраторами		
	4. Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий		
	5. Принятие мер по устранению последствий инцидентов		
	6. Планирование и принятие мер по предотвращению повторного возникновения инцидентов		
Управление конфигурацией информационной системы ПДн и системы защиты персональных данных	1. Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы ПДн и системы защиты персональных данных		
	2. Управление изменениями конфигурации информационной системы ПДн и системы защиты персональных данных		
	3. Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы ПДн и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		
	4. Документирование информации (данных) об изменениях в конфигурации информационной системы ПДн и системы защиты персональных данных		

Подпись руководителя подразделения Общества \_\_\_\_\_ (И.О. Фамилия)

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

Перечень персональных данных, обрабатываемых в АО «ТЭК-Торг»  
в ИСПДн

(название АИС, если автоматизированная обработка)

Подразделение, осуществляющее обработку персональных данных (далее – ПДн)	Цель обработки ПДн	Состав ПДн										Количество субъектов ПДн	Срок обработки	Необходимость согласия субъекта ПДн
		О.И.Ф.	телефон	.....	.....	.....	.....	.....	.....	.....	.....			

Журнал учета носителей персональных данных

(наименование структурного АО «ТЭК-Торг»)

№ п/п	Дата создания	Тип носителя	Учетный номер	Место хранения	Категория персональных данных	Цель обработки	Роспись создателя	Отметка об уничтожении

**УТВЕРЖДЕНА**

Генеральным директором АО «ТЭК-Торг»

«10» сентября 2018 г.

(Приказ № 50 от 10 . 09 . 2018)



Д.А. Сытин

## **ПОЛОЖЕНИЕ**

о работе с персональными данными работников АО «ТЭК-Торг»  
(вторая редакция)

Москва, 2018

## Содержание

1. Общие положения.....	3
2. Получение и обработка персональных данных работников.....	4
3. Защита персональных данных работников.....	5
4. Передача и распространение персональных данных работников.....	6
5. Права и обязанности работников в отношении своих персональных данных.....	7
6. Контроль соблюдения режима работы с персональными данными .....	7
Приложение № 1.....	9
Согласие на обработку персональных данных	
Приложение № 2.....	11
Журнал учета выдачи информации о персональных данных работников АО «ТЭК-Торг»	
Приложение № 3.....	12
Согласие на передачу персональных данных третьей стороне	

## 1. Общие положения

1.1. Настоящее Положение о работе с персональными данными работников АО «ТЭК-Торг» (далее - Положение) определяет порядок получения, обработки, хранения, передачи и любого другого использования персональных данных работников АО «ТЭК-Торг» с учетом требований Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», иных нормативных правовых актов, определяющих случаи и особенности обработки персональных данных.

1.2. В настоящем Положении используются следующие основные понятия и сокращения:

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

**ПДн (персональные данные)** - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

**Использование ПДн** - действия (операции) с ПДн, совершаемые Обществом в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц.

**Общество, Работодатель** – АО «ТЭК-Торг».

**Конфиденциальность ПДн** - обязательное для соблюдения Обществом или иным получившим доступ к ПДн лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

**Работники** - лица, выполняющие в АО «ТЭК-Торг» работу по трудовому договору.

**Обезличивание ПДн** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн к конкретному субъекту 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.

**Общедоступные ПДн** - ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе.

**ОИБ** – Отдел информационной безопасности АО «ТЭК-Торг».

**ОРП** - Отдел по работе с персоналом АО «ТЭК-Торг».

**Распространение ПДн** – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

**РФ** - Российская Федерация.

**Трансграничная передача ПДн** - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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

**ТК РФ** - Трудовой кодекс РФ.

1.3. Защита ПДн Работника от неправомерного их использования или утраты обеспечивается Работодателем за счет средств Работодателя в порядке, установленном ТК РФ, Законом, а также иными нормативными правовыми актами, определяющими случаи и особенности обработки ПДн.

1.4. Лица, виновные в нарушении требований законодательства РФ о защите ПДн, а также настоящего Положения, несут гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством РФ.

## **2. Получение и обработка персональных данных работников**

- 2.1. ПДн Работника подлежат обработке Работодателем в связи с трудовыми отношениями.
- 2.2. Обработка ПДн Работников осуществляется с учетом принципов, установленных статьей 5 Закона, исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия Работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности Работников, контроля количества и качества выполняемой работы, обеспечения сохранности имущества, а также с целью реализации страховых программ.
- 2.3. Объем и содержание получаемых и обрабатываемых ПДн Работника определяются Обществом в соответствии с Конституцией РФ, ТК РФ, иными федеральными законами и нормативными правовыми актами, определяющими случаи и особенности обработки ПДн, а также международными договорами.
- 2.4. Общество получает ПДн непосредственно от самого Работника.
- 2.5. В случаях, предусмотренных Законом, Общество получает от Работника письменное согласие на обработку ПДн по форме Приложения № 1.
- 2.6. Работодатель должен сообщить Работнику о целях, предполагаемых источниках и способах получения ПДн, а также о характере ПДн, подлежащих обработке, и последствиях отказа Работника дать письменное согласие на их обработку.
- 2.7. Перечень ПДн Работников, обрабатываемых в Обществе, определяется в общем перечне ПДн, обрабатываемых в Обществе, в соответствии с требованиями «Политики в области обработки персональных данных АО «ТЭК-Торг».
- 2.8. Документы, содержащие ПДн Работников, хранятся в делах ОРП и бухгалтерии Общества.
- 2.9. В случае изменений ПДн Работник обязан в течение 3 (трех) рабочих дней сообщить об этом в ОРП.
- 2.10. В случае выявления недостоверных ПДн Работника или неправомерных действий Работодателя с ними при обращении или по запросу Работника, являющегося субъектом ПДн (его законного представителя либо уполномоченного органа по защите прав субъектов ПДн), Общество осуществляет блокирование ПДн, относящихся к соответствующему работнику, с момента такого обращения или получения такого запроса на период проверки.
- 2.11. В случае подтверждения факта недостоверности ПДн Работника Общество уточняет ПДн и прекращает их блокирование на основании документов, представленных Работником, являющимся субъектом ПДн, или его законным представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов.
- 2.12. В случае выявления неправомерных действий Работодателя с ПДн в срок, не превышающий 3 (три) рабочих дня с даты такого выявления, Работодатель устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений Общество в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерности действий с ПДн, уничтожает ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Общество уведомляет Работника, являющегося субъектом ПДн, или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.



- 2.13. Если обработка ПДн Работника осуществляется в целях, отличных от целей исполнения трудового договора, то у Работника берется письменное согласие на обработку ПДн по форме, указанной в Приложении № 1 к настоящему Положению, за исключением случаев, предусмотренных частью 2 статьи 6 Закона. Работник принимает решение о предоставлении своих ПДн и дает согласие на их обработку по своей воле и в своем интересе.
- 2.14. Согласие на обработку ПДн может быть отозвано Работником. В этом случае Общество прекращает обработку соответствующих ПДн и уничтожает их в срок, не превышающий 30 (тридцати) дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Работодателем и соответствующим Работником. Об уничтожении ПДн Работодатель уведомляет Работника.
- 2.15. При принятии решений, затрагивающих интересы Работника, руководитель Общества не имеет права основываться на ПДн Работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. В случае, если на основании ПДн Работника невозможно достоверно установить какой-либо факт, Работнику может быть предложено представить письменные разъяснения.
- 2.16. Работодатель не имеет права получать и обрабатывать персональные данные Работника о его членстве в общественных объединениях или его профсоюзной деятельности, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных ТК РФ и иными федеральными законами.
- 2.17. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ руководитель Общества вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.
- 2.18. При сборе ПДн, а также при обращении Работника к Работодателю либо при получении Работодателем запроса от Работника (его законного представителя) Работодатель обязан осуществлять действия в соответствии со статьями 18 и 20 Закона.

### **3. Защита персональных данных Работников**

- 3.1. Обществом и третьими лицами, получающими доступ к ПДн Работников, обеспечивается конфиденциальность таких данных, за исключением:
- обезличенных ПДн;
  - общедоступных ПДн.
- 3.2. При обработке ПДн Общество принимает необходимые организационные и технические меры (в том числе использует шифровальные (криптографические) средства) для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий с учетом действия статьи 19 Закона и раздела 3 настоящего Положения.
- 3.3. В Обществе организация работ по защите ПДн регламентируется внутренним документом, утвержденным в соответствии с действующим в Обществе порядком.
- 3.4. Генеральный директор Общества утверждает список Работников, доступ которых к ПДн необходим для выполнения их должностных обязанностей и несет ответственность в соответствии с законодательством РФ за нарушение режима защиты этих ПДн.
- 3.5. В соответствии с ТК РФ ПДн Работников подлежат защите от неправомерного доступа, использования или утраты. С этой целью хранение ПДн Работников осуществляется Работодателем в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

- 3.6. Ведение личных дел Работников с их ПДн осуществляет ОРП, Работники которого несут ответственность за конфиденциальность ПДн и их правомерное использование.
- 3.7. ПДн Работников хранятся в бумажном виде в папках в составе личных дел Работников в ОРП в закрывающемся на ключ металлическом шкафу, обеспечивающем защиту от несанкционированного доступа.
- 3.8. Запрещается помещать в папку с личным делом Работника ПДн иных субъектов, за исключением близких родственников этого Работника.
- 3.9. Личные карточки Т-2 и трудовые книжки Работников хранятся в закрывающемся на ключ металлическом шкафу в помещении ОРП.
- 3.10. В отсутствие ответственных Работников помещения ОРП закрываются на ключ.
- 3.11. Личные карточки Т-2 и личные дела уволенных Работников формируются и подшиваются в дела и сдаются на архивное хранение в установленном порядке.
- 3.12. ПДн Работников могут также храниться в электронном виде в информационной системе Общества.
- 3.13. Доступ к информационной системе ПДн Работников обеспечивается через двухуровневую систему паролей (для доступа к локальной сети и непосредственно к базе данных) в порядке, действующем в Обществе.
- 3.14. Доступ к ПДн Работников имеют:
- Генеральный директор Общества, Работники ОРП и бухгалтерии - к ПДн всех Работников;
  - руководители структурных подразделений Общества – к ПДн Работников подчиненных им структурных подразделений Общества.
- 3.15. Допуск к ПДн Работников другим категориям Работников осуществляется только с разрешения Генерального директора Общества.
- 3.16. В соответствии с частью 4 статьи 21 Закона в случае достижения цели обработки ПДн Общество незамедлительно прекращает их обработку и уничтожает их в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки соответствующих ПДн, если иное не предусмотрено федеральными законами и настоящим Положением, после чего уведомляет об этом Работника или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПД, - также в указанный орган.
- 3.17. ПДн Работников уничтожаются с учетом требований законодательства РФ и настоящего раздела Положения:
- в электронном виде - Работниками ОРП и бухгалтерии либо на основании их заявки системными администраторами Технического отдела Общества;
  - в бумажном виде - в установленном в Обществе порядке выделения дел к уничтожению, либо в ином порядке по указанию (распоряжению) Генерального директора Общества.

#### **4. Передача и распространение персональных данных Работников**

- 4.1. Информация, относящаяся к ПДн Работников, может быть предоставлена органам государственной власти в порядке, установленном федеральным законодательством.
- 4.2. Передача третьим лицам ПДн Работника осуществляется только с письменного согласия субъекта, которое оформляется по форме, указанной в Приложении № 3 к настоящему Положению, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника, а также в случаях, установленных федеральным законодательством.
- 4.3. Работодатель не может сообщать ПДн Работника в коммерческих целях без его письменного согласия.
- 4.4. Работодатель может передавать ПДн Работника его представителям в порядке, установленном ТК РФ и иными федеральными законами, и ограничивать эту информацию

только теми ПДн Работника, которые необходимы для выполнения указанными представителями их функций.

4.5. Если ПДн Работника передаются третьим лицам с целью выполнения договора между Обществом и лицом, которому передаются ПДн, то в таком договоре должны быть прописаны обязательства сторон по обеспечению конфиденциальности и безопасности обрабатываемых ПДн.

4.6. При передаче ПДн предусматриваются адекватные меры защиты от несанкционированного доступа и искажения (утери) ПДн.

4.7. В ОРП ведется Журнал учета предоставленных ПДн Работников в соответствии с формой, указанной в Приложении № 2 к настоящему Положению, в котором регистрируются запросы, фиксируются сведения о лице, направившем запрос, дата предоставления ПДн или дата уведомления об отказе в предоставлении ПДн, а также отмечается, какая именно информация была передана.

4.8. Распространение ПДн Работников с возможностью ознакомления с ними неограниченного круга лиц (в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом) осуществляется в строгом соответствии с требованиями законодательства РФ на основании письменного согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.

## **5. Права и обязанности Работников в отношении своих персональных данных**

5.1. Работники обязаны предоставлять Работодателю актуальные ПДн.

5.2. В соответствии со статьей 89 ТК РФ Работники имеют право на:

- полную информацию о своих ПДн и обработке этих данных;
- свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей его ПДн (например, копии трудовой книжки, приказов о приеме, переводе) за исключением случаев, предусмотренных законодательством РФ;
- определение представителей для защиты своих ПДн;
- доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;
- требование об исключении или исправлении Работодателем неверных или неполных ПДн, а также данных, обработанных с нарушением требований законодательства РФ. При отказе Работников ОРП исключить или исправить ПДн Работника он имеет право заявить в письменной форме Работодателю о своем несогласии с соответствующим обоснованием такого несогласия. ПДн оценочного характера Работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- извещение Работодателем всех лиц, которым ранее были сообщены неверные или неполные ПДн Работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суде любых неправомерных действий или бездействия Работодателя при обработке и защите его ПДн.

5.3. Работники должны быть ознакомлены с настоящим Положением под распись.

## **6. Контроль соблюдения режима работы с персональными данными**

В Обществе проводятся регулярные проверки соблюдения требований Закона и связанных с ним нормативных актов.

Для расследования случаев нарушения требований по работе с ПДн Генеральным директором Общества могут назначаться внеплановые проверки, а также служебные расследования.

**Приложение № 1**  
**к Положению «О работе с персональными**  
**данными работников АО «ТЭК-Торг»**

**СОГЛАСИЕ**  
**НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Я, (ФИО полностью) \_\_\_\_\_,

зарегистрированный по адресу: \_\_\_\_\_

\_\_\_\_\_ ,  
 паспорт (удостоверение личности \_\_\_\_\_) серии \_\_\_\_\_

№ \_\_\_\_\_ выдан \_\_\_\_\_

\_\_\_\_\_ « \_\_\_\_\_ » \_\_\_\_\_ г.

в соответствии с требованиями статьи 9 Федерального закона от 27.07.06 № 152-ФЗ «О персональных данных», **передаю свои персональные данные** (далее – ПДн) **и даю согласие на их обработку** с использованием и без использования средств автоматизации в АО «ТЭК-Торг» (далее Общество), зарегистрированном по адресу: г. Москва, улица Тимура Фрунзе, дом 24.

Цели обработки, состав данных, сроки действия и порядок отзыва данного согласия, определены в таблице ниже:

№	Цель обработки	Состав ПДн	Срок обработки (С момента подписания согласия)	Порядок отзыва согласия
1.	Формирование общедоступной справочной информации	Общедоступные ПДн: Фамилия, имя, отчество; дата рождения (без указания года); место работы и должность; служебный телефон; адрес служебной электронной почты	В течение всего срока действия трудового договора	Согласие на обработку моих ПДн может быть отозвано мною в любое время в течение срока действия согласия путем направления в АО «ТЭК-Торг» в письменном виде уведомления об отзыве согласия в произвольной форме. Обработка ПДн будет прекращена и ПДн будут уничтожены в течение трех рабочих дней со дня получения письменного заявления об отзыве
2.	Бронирование гостиниц и проездных документов	Фамилия, имя, отчество; дата рождения; паспортные данные; место работы и должность	В течение всего срока действия трудового договора	Согласие на обработку моих ПДн может быть отозвано мною в любое время в течение срока действия согласия путем направления в АО «ТЭК-Торг» в

				<p>письменном виде уведомления об отзыве согласия в произвольной форме.</p> <p>Обработка ПДн будет прекращена и ПДн будут уничтожены в течение трех рабочих дней со дня получения письменного заявления об отзыве</p>
3.	Организация обучения, повышения квалификации, семинаров, вебинаров, тренингов, конференций	Фамилия, имя, отчество; дата рождения; паспортные данные; место работы и должность	В течение всего срока действия трудового договора	<p>Согласие на обработку моих ПДн может быть отозвано мною в любое время в течение срока действия согласия путем направления в АО «ТЭК-Торг» в письменном виде уведомления об отзыве согласия в произвольной форме.</p> <p>Обработка ПДн будет прекращена и ПДн будут уничтожены в течение трех рабочих дней со дня получения письменного заявления об отзыве</p>
4.	Управление персоналом	Фамилия, имя отчество, пол, дата и место рождения, гражданство, паспортные данные, реквизиты документа, удостоверяющего личность, СНИЛС, ИНН, имеемые аттестаты и сертификаты, образование, специальность, профессия, доходы, стаж работы, предыдущее место работы и зарплата, состояние в браке, состав семьи, адрес регистрации, адрес места жительства, домашний телефон, марка и госномер личного автомобиля, реквизиты и данные из военного билета, знание иностранного языка	В течение всего срока действия трудового договора	<p>Согласие на обработку моих ПДн может быть отозвано мною в любое время в течение срока действия согласия путем направления в АО «ТЭК-Торг» в письменном виде уведомления об отзыве согласия в произвольной форме.</p> <p>Обработка ПДн будет прекращена и ПДн будут уничтожены в течение трех рабочих дней со дня получения письменного заявления об отзыве</p>

Настоящее согласие распространяется на сбор, систематизацию, накопление, хранение, запись на электронные носители и их хранение, уточнение, обновление, изменение, использование (в том числе предоставление в случаях, прямо предусмотренных целями обработки и действующим законодательством РФ), обезличивание, блокирование, уничтожение и иные способы обработки.

Последствия отказа от дачи согласия на обработку моих персональных данных мне разъяснены.

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

Подпись

ФИО

**Приложение № 2**  
**к Положению «О работе с персональными**  
**данными работников АО «ТЭК-Торг»**

**ЖУРНАЛ**

**учета выдачи информации о персональных данных работников АО «ТЭК-Торг»**

Начат: «\_\_» \_\_\_\_\_ 20\_\_ г.

Окончен: «\_\_» \_\_\_\_\_ 20\_\_ г.

Дата поступления запроса, наименование организации	Содержание запроса	Дата передачи информации/отказа в предоставлении информации	Перечень предоставленной информации	Дата и номер исходящего письма

Приложение № 3  
к Положению «О работе с персональными  
данными работников АО «ТЭК-Торг»

СОГЛАСИЕ  
НА ПЕРЕДАЧУ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬЕЙ СТОРОНЕ

Я, (ФИО полностью) \_\_\_\_\_,  
зарегистрированный по адресу: \_\_\_\_\_

паспорт (удостоверение личности \_\_\_\_\_) серии \_\_\_\_\_  
№ \_\_\_\_\_ выдан \_\_\_\_\_  
\_\_\_\_\_ «\_\_\_» \_\_\_\_\_ г.

в соответствии с требованиями статьи 9 Федерального закона от 27.07.06 № 152-ФЗ «О  
персональных данных», даю согласие на передачу моих персональных данных (далее – ПДн) на  
обработку с использованием и без использования средств автоматизации в

(наименование учреждения, адрес места положения)

Цели обработки, состав данных, сроки действия и порядок отзыва данного согласия, определены в  
таблице ниже:

№	Цель обработки	Состав ПДн	Срок обработки (С момента подписания согласия)	Порядок отзыва согласия
1.				Согласие на обработку моих ПДн может быть отозвано мною в любое время в течение срока действия согласия путем направления в АО «ТЭК- Торг» в письменном виде уведомления об отзыве согласия в произвольной форме. Обработка ПДн будет прекращена и ПДн будут уничтожены в течение трех рабочих дней со дня получения письменного заявления об отзыве

Настоящее согласие распространяется на сбор, систематизацию, накопление, хранение, запись на  
электронные носители и их хранение, уточнение, обновление, изменение, использование (в том  
числе предоставление в случаях, прямо предусмотренных целями обработки и действующим  
законодательством РФ), обезличивание, блокирование, уничтожение и иные способы обработки.

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

Подпись

ФИО



**УТВЕРЖДЕНА**

Генеральным директором АО «ТЭК-Торг»

«10» сентября 2018 г.

(Приказ № 50 от 10. 09. 2018)

 Д.А. Сытин

**РЕГЛАМЕНТ**  
**работы с запросами и обращениями субъектов персональных данных**  
**и уполномоченных органов по защите прав субъектов персональных**  
**данных, обрабатываемых в АО «ТЭК-Торг»**  
**(вторая редакция)**

**Москва 2018 г.**

## **1. Общие положения**

1.1. Настоящий Регламент работы с запросами и обращениями субъектов персональных данных и уполномоченных органов по защите прав субъектов персональных данных, обрабатываемых в АО «ТЭК-Торг» (далее по тексту – Регламент), разработан в целях соблюдения прав субъектов персональных данных и установления порядка обработки запросов и обращений субъектов персональных данных, а также уполномоченных органов по защите прав субъектов персональных данных (далее – запросы и обращения).

1.2. Регламент разработан в соответствии с Федеральным законом от 27.06.2006 № 152-ФЗ «О персональных данных», нормативно-правовыми актами Российской Федерации в области защиты персональных данных и внутренними документами АО «ТЭК-Торг».

## **2. Права субъектов персональных данных**

2.1. Субъект персональных данных вправе требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2.2. Субъект персональных данных при обращении или при направлении запроса имеет право на получение информации, касающейся обработки его персональных данных в АО «ТЭК-Торг», в том числе содержащей:

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые способы обработки персональных данных;
- наименование и место нахождения АО «ТЭК-Торг», сведения о лицах (за исключением работников АО «ТЭК-Торг»), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с АО «ТЭК-Торг» или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законодательством;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению АО «ТЭК-Торг», если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные федеральными законами.

2.3. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает конституционные права и свободы других лиц.

### **3. Порядок обработки обращений**

3.1. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю при его обращении в АО «ТЭК-Торг», либо при получении от субъекта персональных данных или его законного представителя соответствующего запроса.

3.2. Запрос и обращение должны содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя.

3.3. Запрос и обращение могут быть направлены в электронной форме и подписаны электронной подписью в соответствии с законодательством Российской Федерации.

3.4. В АО «ТЭК-Торг» к рассмотрению не принимаются запросы и обращения, не содержащие всех необходимых сведений, указанных в пунктах 3.2. и 3.3. Регламента.

3.5. Ответ субъекту персональных данных или его законному представителю направляется в течение десяти рабочих дней с момента получения запроса.

3.6. Субъекту персональных данных или его законному представителю в течение десяти рабочих дней с момента получения запроса предоставляется возможность ознакомления с персональными данными, если их права соответствующим образом подтверждены и нет законодательных ограничений на доступ к такой информации.

3.7. Сведения должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

3.8. В случае, если сведения, указанные в пункте 2.2. Регламента а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в АО «ТЭК-Торг» или направить ему повторный запрос в целях получения сведений, указанных в пункте 2.2.Регламента, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

3.9. Субъект персональных данных вправе обратиться повторно в АО «ТЭК-Торг» или направить повторный запрос в целях получения сведений, указанных в пункте 2.2 Регламента, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 3.8. Регламента, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального

обращения. Повторный запрос наряду со сведениями, указанными в пункте 2.2 Регламента, должен содержать обоснование направления повторного запроса.

3.10. АО «ТЭК-Торг» вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 3.8. и 3.9. Регламента. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на АО «ТЭК-Торг».

3.11. В случае отказа в предоставлении субъекту персональных данных или его законному представителю информации о наличии персональных данных, а также таких персональных данных, дается в письменной форме мотивированный ответ, содержащий ссылку на положение части 5 статьи 14 Федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных или его законного представителя, либо с даты получения запроса субъекта персональных данных или его законного представителя.

3.12. Предоставление субъекту персональных данных или его законному представителю возможности ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внесение в них необходимых изменений, уничтожение или блокирование соответствующих персональных данных по предоставлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработка которых осуществляется, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки осуществляется безвозмездно. О внесенных изменениях и предпринятых мерах уведомляются: субъект персональных данных или его законный представитель, а также третьи лица, которым персональные данные этого субъекта были переданы.

3.13. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных АО «ТЭК-Торг» обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению АО «ТЭК-Торг») с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных АО «ТЭК-Торг» обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению АО «ТЭК-Торг») с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.14. В случае подтверждения факта неточности персональных данных АО «ТЭК-Торг» на основании сведений, представленных субъектом персональных данных или его

представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению АО «ТЭК-Торг») в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.15. В случае выявления неправомерной обработки персональных данных, осуществляемой в АО «ТЭК-Торг» или лицом, действующим по поручению АО «ТЭК-Торг», в срок, не превышающий трех рабочих дней с даты этого выявления, АО «ТЭК-Торг» обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению АО «ТЭК-Торг». В случае, если обеспечить правомерность обработки персональных данных невозможно, АО «ТЭК-Торг» в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных АО «ТЭК-Торг» обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

#### **4. Полномочия ответственного лица в процессе обработки обращений и запросов**

4.1. Ответственность за обработку запросов и обращений и подготовку ответов возлагается на лицо, ответственное за обработку персональных данных (далее – Ответственное лицо).

4.2. Поступившие в АО «ТЭК-Торг» запросы и обращения регистрирует в соответствии с принятым в АО «ТЭК-Торг» порядком документооборота и передаются Ответственному лицу.

4.3. Запросы и обращения, требующие правовой оценки, в том числе связанные с судебными разбирательствами, передаются на рассмотрение в Юридический отдел АО «ТЭК-Торг».

4.4. Ответственным лицом ведется «Журнал учета запросов и обращений в АО «ТЭК-Торг» субъектов персональных данных, а также уполномоченного органа по защите прав субъектов персональных данных» по форме Приложения к Регламенту (далее по тексту – Журнал).

4.5. В Журнале фиксируется следующая информация: сведения о запрашивающем лице, краткое содержание обращения, цель запроса, отметка о предоставлении информации или отказе в её предоставлении, дата предоставления информации / отказа в предоставлении информации, подпись ответственного лица, примечание.

4.6. Журнал хранится у Ответственного лица.

## **5. Актуализация документа**

5.1. Регламент пересматривается не реже одного раза в три года, а также при изменении законодательства Российской Федерации, по инициативе Генерального директора АО «ТЭК-Торг» или Отдела информационной безопасности АО «ТЭК-Торг».

# ЖУРНАЛ

учета запросов и обращений в АО «ТЭК-Торг» субъектов персональных данных, а также уполномоченного органа по защите прав субъектов персональных данных

Журнал начат «\_\_» \_\_\_\_\_ 201\_\_ г.

Журнал завершён «\_\_» \_\_\_\_\_ 201\_\_ г.

Должность \_\_\_\_\_

Должность \_\_\_\_\_

ФИО лица \_\_\_\_\_

ФИО лица \_\_\_\_\_

На \_\_\_\_\_ листах

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в её предоставлении	Дата предоставления информации / отказа в предоставлении информации	Подпись ответственного лица	Примечание