Акционерное общество
коммунальных электрических сетей Саратовской области
ОБЛКОММУНЭНЕРГО

УТВЕРЖДАЮ
И.о. генерального директора
_____/Р.Х. Хаметов/
"05" 10 2021 г.

ПОЛОЖЕНИЕ

О порядке организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в АО «Облкоммунэнерго»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение документа

1.1.1. Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – Положение) определяет содержание и порядок осуществления мероприятий по защите персональных данных в АО «Облкоммунэнерго» (далее – Общество, оператор).

1.1.2. Настоящее Положение разработано на основании Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 30 декабря 2020 г. N 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», Федерального закона от 25.07.2011 N 261-ФЗ « О внесении изменений в Федеральный закон «О персональных данных», Постановления Правительства Российской
Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. N 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 15 февраля 2017 г. N 27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17», приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 24 февраля 2021 г. N 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения» и других нормативно-правовых актов Российской Федерации и «Политики организации обработки и защиты персональных данных в Обществе».

1.1.3. Цель настоящего Положения – регулирование работ по защите персональных данных (далее - ПДн) и обеспечение функционирования информационных систем персональных данных в Обществе в соответствии с требованиями действующего федерального законодательства в области информационной безопасности.

1.2. Область действия документа

1.2.1. Действие Положения распространяется на информационные системы персональных данных Общества, в которых осуществляется обработка персональных данных как с использованием средств автоматизации, так и без использования таковых.

1.2.2. Все сотрудники Общества, допущенные к работе с персональными данными, обрабатываемыми в Обществе, в обязательном порядке должны быть ознакомлены с настоящим Положением под роспись (Приложение №3).

1.3. Вступление в силу документа

1.3.1. Настоящее Положение вступает в силу с момента его утверждения руководителем Общества и действует бессрочно до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом руководителя Общества.

2. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЩЕСТВА

2.1. Планирование работ по обеспечению безопасности персональных данных

2.1.1. В целях исполнения настоящего Положения и на основании Положения о постоянно действующей экспертной комиссии по информационной безопасности (далее – ПДЭК), ПДЭК ежегодно составляет и утверждает у руководителя Общества план работ по обеспечению безопасности персональных данных, обрабатываемых в Обществе.

2.1.2. Проводимые в Обществе мероприятия по обеспечению безопасности персональных данных учитываются ПДЭК в Журнале учета мероприятий по обеспечению безопасности персональных данных в организации по форме, утвержденной настоящим Положением (Приложение № 1).

2.2. Выполнение работ по обеспечению безопасности персональных данных

2.2.1. В целях организации и проведения работ по обеспечению безопасности персональных данных в Обществе приказом руководителя Общества назначаются:

– уполномоченное лицо (ответственный за организацию обработки ПДн в организации), ответственное за проведение мероприятий по обеспечению безопасности персональных данных и поддержание необходимого уровня информационной безопасности;

– специалист по информационной безопасности (ИБ), ответственный за установку, настройку и обслуживание средств защиты информации, применяемых в Обществе для обеспечения безопасности персональных данных, а также за организацию и проведение инструктажа сотрудников по основам информационной безопасности при работе с персональными данными.

2.2.2. Указанные лица, совместно с ПДЭК, отвечают за проведение следующих мероприятий по обеспечению безопасности персональных данных:

– определение и описание информационных систем персональных данных;

– классификацию информационных систем персональных данных;

– определение актуальных угроз безопасности персональных данных;

– проектирование системы защиты персональных данных, включающей организационные, физические и технические меры и средства защиты;

– закупку, установку и настройку технических средств защиты информации;

– внедрение организационных мер и разработку соответствующих регламентов и положений;

– инструктаж и обучение лиц, которые будут использовать средства защиты информации.

2.2.3. Начальники отделов(управлений, филиалов), в которых происходит обработка персональных данных, являются лицами, ответственными за соблюдение требований настоящего Положения и других установленных в Обществе требований в сфере обработки персональных данных.

2.2.4. Для обеспечения безопасности персональных данных в Обществе применяются следующие меры безопасности:

– организационные меры безопасности:

• инструктаж сотрудников по правилам обеспечения безопасности обрабатываемых персональных данных;

• учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;

• мониторинг и реагирование на инциденты информационной безопасности, связанные с персональными данными, включая проведение внутренних проверок, разбирательств и составление заключений;

• постоянный контроль за соблюдением требований по обеспечению безопасности персональных данных (реализуется путем внутренних аудитов);

– меры физической безопасности:

• ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации. Приказом руководителя Общества вводятся в действие перечень помещений, в которых разрешена обработка персональных данных и перечень помещений, в которых разрешено хранение персональных данных на бумажных и электронных носителях, а так же список лиц, имеющих право на доступ в помещения Общества, в которых разрешены хранение и обработка персональных данных на электронных носителях. Лица, не указанные в списке, в том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств), при наличии необходимости могут посещать помещения с ограниченным доступом в сопровождении ответственных лиц;

• размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

• организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

– технические меры безопасности:

• разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

• регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

• резервирование технических средств, дублирование массивов и носителей информации;

• использование защищенных каналов связи;

• предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

2.2.5. Ремонтно-восстановительные работы технических средств обработки информации, на которых производится обработка персональных данных, проводятся под контролем ИБ. В случае необходимости ремонт технических средств может быть проведен с привлечением сторонних специалистов на договорной основе с составлением актов выполненных работ.

2.3. Контроль выполнения работ по обеспечению безопасности персональных данных

2.3.1. Контроль выполнения работ по обеспечению безопасности персональных данных в Обществе (далее – Контроль) осуществляется путем

проведения периодических плановых внутренних контрольных мероприятий и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

2.3.2. В рамках проведения контрольных мероприятий выполняются:

– проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности персональных данных за истекший период;

– проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности персональных данных;

– проверка соответствия перечня лиц, которым предоставлен доступ к персональным данным, фактическому состоянию;

– проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности персональных данных, в соответствии с требованиями эксплуатационной и технической документации;

– инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности персональных данных (при необходимости);

– проверка соответствия моделей угроз для информационных систем персональных данных условиям функционирования данных систем;

– проверка соответствия организационно-распорядительной документации по обеспечению безопасности персональных данных действующим требованиям законодательства РФ, руководящих документов ФСБ России, ФСТЭК России.

2.3.3. Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

2.3.4. Контрольные мероприятия проводятся как периодически в соответствии с планом работ ПДЭК и планом проведения мероприятий по осуществлению внутреннего контроля, так и внепланово по решению руководителя Общества и в случае возникновения инцидентов информационной безопасности.

2.3.5. Внутренние проверки в Обществе в обязательном порядке проводятся в случае выявления следующих фактов:

– нарушение конфиденциальности, целостности, доступности персональных данных;

– халатность и несоблюдение требований к обеспечению безопасности персональных данных;

– несоблюдение условий хранения носителей персональных данных;

– использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/

целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

2.3.6. Задачами внутренней проверки являются:

– установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

– установление лиц, непосредственно виновных в данном нарушении;

– выявление причин и условий, способствовавших нарушению.

2.4. Совершенствование системы защиты персональных данных

2.4.1. Ежегодно ПДЭК направляет руководителю Общества отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности персональных данных, обрабатываемых в Обществе, вместе с перечнем предложений по совершенствованию системы защиты персональных данных.

2.4.2. Необходимость реализации мероприятий по совершенствованию системы защиты персональных данных может быть обусловлена:

– результатами проведенных контрольных мероприятий;

– изменениями федерального законодательства в области персональных данных;

– изменениями структуры процессов обработки персональных данных в Обществе;

– результатами анализа инцидентов информационной безопасности;

– результатами мероприятий по контролю и надзору за обработкой персональных данных, проводимых уполномоченным органом;

– жалоб и запросов субъектов персональных данных.

2.4.3. На основании решения, принятого руководителем Общества по результатам рассмотрения ежегодного отчета и предложений по совершенствованию системы защиты персональных данных, ПДЭК составляет план работ по обеспечению безопасности персональных данных, обрабатываемых в Обществе, на следующий год.

3. ПОРЯДОК ПЕРЕСМОТРА ПОЛОЖЕНИЯ О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕ

Положение подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств информационных систем Общества, приводящих к существенным изменениям технологии обработки информации.

Положение подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за организацию обработки ПДн в организации.

Полный плановый пересмотр данного документа проводится регулярно, раз в год, с целью проверки соответствия положений данного документа реальным условиям применения их в информационных системах Общества.

Частичный пересмотр данного документа проводится по письменному предложению ИБ. Изменения в Положении (сведения о них) фиксируются в Листе регистрации изменений (Приложение №2).

Вносимые изменения не должны противоречить другим положениям данного документа. При получении изменений к данному Положению, руководители подразделений Общества в течение трех рабочих дней вносят свои предложения и/или замечания к поступившим изменениям.

Должность ответственного за обработку ПДн в Обществе	ФИО ответственного за обработку ПДн в Обществе
Заместитель генерального директора по перспективному развитию	Хаметов Р.Х.

Приложение № 1
к Положению по организации и проведению работ
по обеспечению безопасности персональных
данных
при их обработке в информационных системах
персональных данных АО "Облкоммунэнерго"

Журнал учета мероприятий по обеспечению безопасности персональных данных

№ п/п	Наименование мероприятия, основание для проведения	Краткое описание мероприятия	Дата (сроки) проведения мероприятия	Объекты контроля	Ф. И. О. лица, проводившего мероприятие	Подпись лица, проводившего мероприятие
1	2	3	4	5	6	7

Приложение № 2
к Положению по организации и проведению работ
по обеспечению безопасности персональных данных
при их обработке в информационных системах
персональных данных АО "Облкоммунэнерго"

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В ПОЛОЖЕНИИ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБЩЕСТВА

№ п/п	Дата	Внесенное изменение	Основание (наименование, номер и дата документа)	Кем внесено изменение (должность, подпись)