



Акционерное общество
коммунальных электрических сетей Саратовской области

ОБЛКОММУНЭНЕРГО

ПРИКАЗ

г. Саратов

«16» 04 2025 г.

№ 01-01/118

Об утверждении положения «О порядке работы с конфиденциальной информацией в АО «Облкоммунэнерго»

В целях исполнения Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федерального Закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных», Указа Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», и иными нормативно-правовыми актами Российской Федерации, определяющими требования в сфере работы с конфиденциальной информацией, а также в целях обеспечения информационной безопасности АО «Облкоммунэнерго» (далее – Общество)

ПРИКАЗЫВАЮ:

1. Признать утратившим силу Приказ генерального директора Общества от 10.04.2024 г. №01/01/102 «Об утверждении перечня конфиденциальной информации».
2. Утвердить положение «О порядке работы с конфиденциальной информацией» (Приложение №1).
3. Контроль за исполнением настоящего приказа возложить на заместителя генерального директора по перспективному развитию Хаметова Р.Х., ответственного за организацию обработки персональных данных в АО «Облкоммунэнерго».

Генеральный директор

В. Г. Ойкин

Приложение №1
к приказу Об утверждении положения
«О порядке работы с конфиденциальной
информацией в АО «Облкоммунэнерго»

УТВЕРЖДАЮ

Генеральный директор

/В.Г.Ойкин/

" 16 " апреля 2025 г.

ПОЛОЖЕНИЕ

**О порядке работы с конфиденциальной
информацией в АО «Облкоммунэнерго»**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение документа

1.1.1. Положение о порядке работы с конфиденциальной информацией (далее – Положение) определяет содержание и порядок обработки конфиденциальной информации и проведение мероприятий по защите конфиденциальной информации в информационных системах и без применения средств автоматизации в АО «Облкоммунэнерго» (далее – Общество).

1.1.2. Настоящее Положение разработано на основании действующего законодательства Российской Федерации, в том числе на основе Гражданского кодекса Российской Федерации, Трудового кодекса Российской Федерации, Указа Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», Федерального закона Российской Федерации от 27.07. 2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федерального закона Российской Федерации от 27.07.2006. № 152-ФЗ «О персональных данных» и иных нормативно-правовых актов Российской Федерации, определяющими требования в сфере работы с конфиденциальной информацией.

1.1.3. Цель настоящего Положения – регулирование обработки конфиденциальной информации (далее – КИ) и обеспечение функционирования информационных систем, в которых производится обработка КИ 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 сотрудников общества, принимающих участие в документообороте Общества, и информационные системы Общества, в которых осуществляется обработка КИ как с использованием средств автоматизации, так и без использования таковых.

1.2.2. Настоящее Положение должно быть размещено на информационных ресурсах Общества: сайтах — <https://www.oao-oke.ru/> и <http://site> для беспрепятственного ознакомления всеми сотрудниками Общества, допущенными к работе с КИ в Обществе.

1.3. Вступление в силу документа

1.3.1. Настоящее Положение вступает в силу с момента его утверждения генеральным директором Общества и действует бессрочно.

1.3.2. Все изменения и дополнения в Положение вносятся приказом генеральным директором Общества.

2. ПОНЯТИЯ И ТЕРМИНЫ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ПОЛОЖЕНИИ

2.1. Термины, применяемые в настоящем Положении, означают следующее:

информация ограниченного доступа – информация, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничен федеральными законами, актами Президента Российской Федерации и локальными актами Общества;

обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

доступ к информации - возможность получения информации и ее использования;

конфиденциальность информации ограниченного доступа - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

конфиденциальная информация – информация ограниченного доступа, доступ к которой ограничивается обладателем в соответствии с федеральными законами, актами Президента Российской Федерации и локальными актами Общества и включает в себя, в том числе, персональные данные, служебную информацию ограниченного распространения;

конфиденциальность информации — обязательное для соблюдения сторонами требование не передавать такую информацию третьим лицам без согласия ее обладателя;

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

обезличенные персональные данные — данные, на основании которых невозможно определить их принадлежность конкретному субъекту персональных данных;

общедоступные персональные данные — персональные данные, размещенные в общедоступных источниках с письменного согласия субъекта персональных данных (общедоступные персональные данные могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов);

информационная система—совокупность информации, содержащейся в базе данных, а также информационных технологий и технических средств,

позволяющих осуществлять обработку такой информации с использованием средств автоматизации или без использования таких средств;

обработка информации — действия (операции) с информацией, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение;

предоставление информации — передача информации в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией;

распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

блокирование информации — временное прекращение сбора, систематизации, накопления, использования, распространения информации, в том числе её передачи;

уничтожение информации — действия, в результате которых невозможно восстановить содержание информации в информационной системе или в результате которых уничтожаются материальные носители с информацией;

допуск к сведениям, составляющих конфиденциальную информацию — процедура оформления права доступа работника Общества к ознакомлению и работе с информацией, являющейся конфиденциальной;

разглашение конфиденциальной информации — действие или бездействие, в результате которых информация, имеющая режим конфиденциальности, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации.

3. ПЕРЕЧЕНЬ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОБЩЕСТВЕ

№ п/п	Наименование
Информация, связанная с оказанием услуг	
1	Сведения, полученные из органов государственной власти, предприятий, организаций и учреждений с условиями дальнейшего неразглашения
2	Информация, отнесенная гражданами к категории «конфиденциальная» и сообщенная ими представителю Общества в качестве необходимой
3	Сведения, на конфиденциальности которых настаивает хотя бы одна из договаривающихся сторон

4	Сведения о заключаемых и исполняемых договорах по предоставлению услуг Обществом и предложениях сторонних организаций, в которых содержатся персональные данные
5	Виды услуг, оказываемые Обществом конкретному гражданину или конкретной сторонней организации
6	Сведения из технической документации в случае, если на их распространение нет согласия правообладателя
Информация технического характера	
7	Сведения, раскрывающие фактическое состояние защиты или методы реализации защиты информации в Обществе
8	Сведения о проводимых, планируемых мероприятиях в Обществе по выявлению технических каналов утечки информации, о применяемых методах, приемах и средствах инструментального контроля защиты информации, результатах обследования объектов защиты, проверки помещений и технических средств в Обществе
9	Состав и характеристики технических средств, применяемых при проведении работ в Обществе в целях уставной деятельности
10	Сведения о существующей системе охраны, пропускном режиме, установленных инженерно-технических средствах охраны в Обществе
11	Сведения о методах защиты информации от утечки, искажения или несанкционированного доступа в процессе ее обработки, хранения в автоматизированных системах управления и средствах вычислительной техники в Обществе
12	Сведения о защищаемых информационных ресурсах: исходные тексты разрабатываемых в интересах организации программ для ЭВМ (баз данных) и алгоритмы их работы, значения паролей, применяемых организации для разграничения доступа и защиты информации, сведения о системе разграничения доступа к информации, правах пользователей, ограничениях на использование информационных ресурсов в Обществе
Информация экономического характера	
13	Планы, программы развития Общества и другие сведения, касающиеся перспективного планирования деятельности, за исключением информации, которую генеральный директор Общества счел возможным использовать в целях формирования положительного имиджа Общества (паблик рилейшнз)
14	Состояние банковского счёта Общества

15	Сведения, касающиеся предмета договора, хода его исполнения, и полученных результатов (объем сведений, признаваемых конфиденциальными, определяется в каждом случае в Соглашении о конфиденциальности)
16	Сведения о финансовом положении и платежеспособности организаций, учреждений, предприятий, сотрудничающих с Обществом
17	Сведения, полученные пользователем по договору коммерческой концессии, раскрывающие секреты производства правообладателя
18	Сведения о партнерах Общества, указанные в соглашениях о конфиденциальности, и состояние деловых отношений с партнерами
Информация о сотрудниках и клиентах (персональные данные)	
19	Сведения о сотрудниках и клиентах (физических лицах), получаемые и обрабатываемые в Обществе (персональные данные)
Служебная информация ограниченного распространения	
20	Информация не отнесенная к категории «государственная тайна», касающаяся деятельности Общества, ограничения на распространение которой диктуются служебной необходимостью – имеющая гриф «Для служебного пользования».
21	Информация об используемых в Обществе средствах криптографической защиты информации, составе средств СКЗИ, порядке применения, перечне средств, местах хранения ключевых носителей
22	Информация о структуре и составе критической информационной инфраструктуры Общества, типах и видах оборудования, используемого на объектах КИИ, методах и способах защиты объектов КИИ.

4. ПОРЯДОК ДОПУСКА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

4.1. По всем вопросам деятельности Общества допуск к конфиденциальной информации имеет руководитель Общества – Генеральный директор, его заместитель или иное лицо, на которое возложены обязанности по обеспечению информационной безопасности Общества, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

4.2. По вопросам, относящимся к их компетенции, к конфиденциальной информации в Обществе имеют допуск следующие лица:

- заместители генерального директора;
- главный инженер;
- главный бухгалтер;
- сотрудники отдела кадров;
- сотрудники Общества, в трудовом (гражданско-правовом) договоре которых имеется соответствующее условие о неразглашении конфиденциальной информации и ими подписано Обязательство о неразглашении конфиденциальной информации (Приложение №1);
- иные лица, получившие допуск к конфиденциальной информации на основании распоряжения генерального директора Общества в соответствии с настоящим Положением.

4.3. Сотрудник Общества, который в соответствии со своими должностными обязанностями имеет доступ или которому будет открыт доступ к конфиденциальной информации, обязан при приеме на работу, либо по первому требованию руководителя структурного подразделения ознакомиться с настоящим Положением и дать письменное обязательство о неразглашении конфиденциальной информации (Приложение №1). Руководитель структурного подразделения организует ознакомление сотрудников с настоящим Положением и получение от сотрудников письменного обязательства о неразглашении конфиденциальной информации. Подлинники обязательств с подписями сотрудников передаются в отдел кадров.

4.4. Допуск иным лицам предоставляется на определенное время или для выполнения конкретного задания на основании заявления с указанием причины получения определенной информации, а также необходимости копирования с применением технических средств указанной информации.

4.5. Заявление рассматривается генеральным директором Общества. По итогам рассмотрения заявления принимается решение о допуске или отказе в допуске иного лица к запрашиваемой им информации. Решение о допуске или отказе в допуске к конфиденциальной информации оформляется визой генерального директора на заявлении иного лица.

4.6. Общество, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую конфиденциальную информацию. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования конфиденциальной информации и срок предоставления этой информации, если иное не установлено действующим законодательством Российской Федерации.

4.7. Допуск к конфиденциальной информации включает в себя:

- ознакомление работника с законодательством о защите информации, об ответственности за его нарушение и с локальными нормативными актами о защите конфиденциальной информации;

- принятие работником на себя обязанности по обеспечению конфиденциальности информации, полученной при осуществлении своей трудовой функции, а также в течении одного года после прекращения трудовых отношений с Обществом;

- прохождение обучения и проверки знаний требований по обеспечению конфиденциальности защищаемой информации;

- в трудовые (гражданско-правовые) договоры лиц, принимаемых на работу, связанную с получением, обработкой, хранением, передачей и использованием информации ограниченного доступа, включается условие об обеспечении конфиденциальности такой информации;

- при подписании трудового (гражданско-правового) договора с сотрудником сотрудники отдела кадров должны ознакомить сотрудника с настоящим Положением под подпись.

5. МЕРЫ, ПРИНИМАЕМЫЕ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОБЩЕСТВЕ

5.1. Защита конфиденциальной информации в Обществе обеспечивается:

- разработкой и внедрением локальных нормативных актов и инструкций по обеспечению защиты конфиденциальной информации;

- заключением договоров (в том числе трудовых) и соглашений с условием о сохранении и обеспечении конфиденциальности информации;

- ограничением доступа к отдельным категориям конфиденциальной информации (информация о средствах криптографической защиты, персональные данные, сведения о объектах критической информационной инфраструктуры), оформлением допуска к такой информации, а также осуществлением учета лиц, получающих доступ к такой информации;

- организацией работы сотрудников с конфиденциальной информацией, в том числе с материальными носителями такой информации;

- установкой уровней (групп, классов) конфиденциальности отдельных видов конфиденциальной информации (персональные данные, сведения о объектах критической информационной инфраструктуры);

- обучением и проверкой знаний по обеспечению режима конфиденциальности информации (для отдельных видов КИ - персональные данные, сведения о объектах критической информационной инфраструктуры, средства криптографической защиты информации);

- применением необходимых технических мер, направленных на ограничение доступа посторонних лиц к конфиденциальной информации.

- применением специализированного программного обеспечения - автоматизированной информационной системы защиты от утечек

информации, в которой осуществляется контроль и управление инцидентами информационной безопасности, контроль за использованием конфиденциальной информации с использованием средств автоматизации и действия сотрудников Общества при обработке конфиденциальной информации.

5.2. Общество имеет право защищать свою конфиденциальную информацию, определяя перечень конфиденциальной информации и правила работы с ней. Средства обработки информации, переданные сотруднику Общества для выполнения своих должностных обязанностей, а также созданная с их помощью информация, является собственностью Общества. В соответствии с этим руководство Общества имеет право использовать автоматизированную информационную систему защиты от утечек информации.

5.3. Компьютерное оборудование, каналы связи и иное имущество, относящееся к информационно-коммуникационной инфраструктуре Общества может быть использовано сотрудниками только и исключительно в служебных целях.

5.3. Сотрудникам Общества запрещается хранить личную информацию на корпоративных ресурсах (рабочие места и общие ресурсы для хранения информации) и передавать ее по корпоративным каналам связи (электронная почта, сеть Интернет и другие), а также использовать в личных целях мессенджеры (программа для мгновенного обмена текстовыми сообщениями и мультимедиа между зарегистрированными пользователями через интернет) любого вида на устройствах информационно-коммуникационной сети Общества.

Настоящее правило подтверждает отсутствие умысла у руководства Общества нарушать неприкосновенность частной жизни сотрудников (статья 137 УК РФ) и нарушение тайны переписки (статья 138 УК РФ), поскольку руководство Общества не может и не должно ожидать, что нарушит право человека на тайну личной переписки или неприкосновенность частной жизни, если получит информацию, относящуюся к рабочей деятельности сотрудника Общества.

Исполнение настоящего правила может контролироваться автоматизированной системой защиты от утечек информации.

5.4. Автоматизированная система защиты от утечек информации может также использоваться для контроля и управления инцидентами информационной безопасности, контроля за использованием информационных ресурсов Общества, предупреждения разглашения или неправомерного использования конфиденциальной информации, защите информационного обмена на объектах критической информационной инфраструктуры, а также для мониторинга трудовой деятельности и анализа работы сотрудников в Обществе, защите законных прав и интересов сотрудников Общества, бережного отношения к имуществу Общества,

соблюдения правил внутреннего трудового распорядка и поддержания трудовой дисциплины в Обществе,

5.5. Обязанности работников по защите конфиденциальной информации

5.5.1 Обеспечивая конфиденциальность, работник обязуется:

- знать и соблюдать требования по получению, обработке, хранению, передаче, конфиденциальной информации, предусмотренные нормативными правовыми актами, коллективным договором, соглашениями, должностной инструкцией, локальными нормативными актами Общества и трудовым (гражданско-правовым) договором;

- производить обработку и передачу (распространение) конфиденциальной информации, перечисленную в п.3 настоящего Положения и иную охраняемую законом тайну, только в целях осуществления своих обязанностей в соответствии с трудовым (гражданско-правовым) договором;

- не использовать конфиденциальную информацию, перечисленную в п.3 настоящего Положения и иную охраняемую законом тайну, в целях, не связанных с осуществлением трудовой деятельности в соответствии с должностными обязанностями;

- не разглашать конфиденциальную информацию, перечисленную в п.3 настоящего Положения и иную охраняемую законом тайну, а также не совершать иных деяний, влекущих уничтожение или утрату такой информации;

- незамедлительно сообщать об утрате или несанкционированном уничтожении конфиденциальной информации своему непосредственному руководителю, а также об иных обстоятельствах, создающих угрозу сохранения конфиденциальности такой информации.

5.5.2. При прекращении трудовых отношений с Обществом сотрудник обязан сдать все материальные носители конфиденциальной информации, а также ключи от помещений и шкафов, в которых они хранятся.

5.6. Ответственность за нарушение конфиденциальности информации

5.6.1. В случае разглашения конфиденциальной информации, ставшей известной работнику в связи с исполнением им своих трудовых обязанностей, в том числе разглашением им персональных данных другого работника, трудовой (гражданско-правовой) договор с работником может быть расторгнут по инициативе работодателя в соответствии с законодательством РФ.

5.6.2. Возмещение ущерба, причиненного Обществу в связи с нарушением правил обработки конфиденциальной информации, производится в установленном законом порядке, организациями и лицами (в том числе работниками Общества), нарушившими действующее законодательство и указанные правила.

5.6.3. Ответственность в соответствии с действующим законодательством, несут также работники и должностные лица Общества, не выполнившие или не обеспечившие выполнение требований настоящего Положения и тем самым способствовавшие нарушению конфиденциальности

информации, а также не принимавшие необходимых и достаточных мер по пресечению ставших им известных фактов нарушения правил обработки конфиденциальной информации в Обществе.

Приложение №1
к Положению о порядке работы с
конфиденциальной информацией в
АО «Облкоммунэнерго»

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации

Я, _____
(Фамилия, имя, отчество)
исполняющий(ая) должностные обязанности по занимаемой должности

(должность, наименование структурного подразделения)
предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностным регламентом, мне будет предоставлен доступ к конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

3. В случае попытки третьих лиц получить от меня конфиденциальную информацию, сообщать непосредственному руководителю.

4. Не использовать конфиденциальную информацию с целью получения личной выгоды.

5. Выполнять требования законодательства РФ и локальных нормативных правовых актов, регламентирующих вопросы защиты конфиденциальной информации.

6. В течение года после прекращения трудового (гражданско-правового) договора не разглашать и не передавать третьим лицам известные мне конфиденциальную информацию.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

Подтверждаю, что ознакомлен(а) с Положением о порядке работы с конфиденциальной информацией в АО «Облкоммунэнерго».

Настоящим подтверждаю, что данные мной обязательства получены на добровольной основе, без принуждения и недопонимания сути данных обязательств.

(подпись) / _____
(расшифровка)
Дата подписания « _____ » _____ 20 _____ г