Акционерное общество
коммунальных электрических сетей Саратовской области
ОБЛКОММУНЭНЕРГО

«03» 07 2025 г. № 01-01/181

ПРИКАЗ

г. Саратов

Об утверждении положения «О порядке эксплуатации автоматизированной системы защиты от утечек информации в АО «Облкоммунэнерго»

В целях исполнения Указа Президента Российской Федерации от 06 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера», Указа Президента Российской Федерации от 1 мая 2022 г. №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Федерального закона Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации», Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» 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. Утвердить положение «О порядке эксплуатации автоматизированной системы защиты от утечек информации» (далее – Положение) (Приложение №1 к приказу).
2. Утвердить перечень должностей сотрудников Общества, на рабочих местах которых предусматривается использование автоматизированной системы защиты от утечек информации (Приложение №1 к Положению)

3. Руководителям структурных подразделений Общества в срок до 30 июля 2025 г. организовать ознакомление подчиненных им сотрудников Общества в соответствии со списком (Приложение №1 к Положению) с Положением, получение от сотрудников подписанных письменных уведомлений об использовании системы защиты от утечек информации (Приложение №2 к Положению) и передачу подлинников уведомлений об использовании системы защиты от утечек информации с личными подписями сотрудников в отдел кадров Общества для хранения в личных делах сотрудников.

4. Начальнику отдела кадров Общества Худошиной О.А. в срок до 30 июля 2025 г. организовать прием и хранение письменных уведомлений сотрудников Общества об использовании системы защиты от утечек информации (в соответствии с перечнем должностей. Приложение №1 к Положению), а также подготовить и в срок до 01 октября 2025 г. внести необходимые изменения в Коллективный договор Общества, а также в трудовые (гражданско-правовые) договора сотрудников Общества путем заключения дополнительных соглашений. (Приложение №3 к Положению)

5. Контроль за исполнением настоящего приказа возложить на заместителя генерального директора Общества по перспективному развитию Хаметова Р.Х.

Генеральный директор **В.Г. Ойкин**

УТВЕРЖДАЮ
Генеральный директор
_____/В.Г.Ойкин/
"03" 07 2025 г.
Приказ № 01-01/181 от 03.07.25г.

ПОЛОЖЕНИЕ

о порядке эксплуатации автоматизированной системы защиты от утечек информации в АО «Облкоммунэнерго»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение документа

1.1.1. Положение о порядке эксплуатации автоматизированной системы защиты от утечек информации (далее – Положение) является локальным документом и определяет правила, характеристики и требования к эксплуатации в АО «Облкоммунэнерго» (далее - Общество) автоматизированной системы защиты от утечек информации (далее – Система).

1.1.2. В развитие изложенных в настоящем Положении требований возможна разработка отдельных организационно-распорядительных документов (инструкции, приказы, положения), конкретизирующих отдельные решения и определяющих правила их применения.

1.1.3. 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 №188 «Об утверждении перечня сведений конфиденциального характера», Указа Президента Российской Федерации от 01.05.2022 №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных», ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности», ГОСТ 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» и иных нормативно-правовых актов Российской Федерации, определяющие требования в сфере работы с конфиденциальной информацией.

1.1.4. Цели и задачи настоящего Положения – регулирование порядка эксплуатации и обеспечения функционирования автоматизированной системы защиты от утечек информации в Обществе в соответствии с требованиями действующего законодательства и локальных актов Общества в области информационной безопасности.

1.2. Область действия документа

1.2.1. Действие Положения распространяется на сотрудников Общества, производящих эксплуатацию и обслуживание Системы и сотрудников Общества, производящих эксплуатацию автоматизированных рабочих мест (далее - АРМ) входящих в информационно-коммуникационную инфраструктуру Общества и находящихся под контролем Системы.

1.2.2. Текст настоящего Положения должен быть размещен на информационных ресурсах Общества: сайтах — https://www.oao-oke.ru/ и

http://site для беспрепятственного ознакомления всеми сотрудниками Общества.

1.2.3. Все сотрудники Общества, допущенные к эксплуатации и обслуживанию Системы, в обязательном порядке должны подписать Обязательство о неразглашении конфиденциальной информации, не содержащей сведений, составляющих государственную тайну (Приложение №4 к Положению) в течении 3 (трех) рабочих дней с момента начала эксплуатации Системы и передано в отдел кадров для хранения в личных делах сотрудников.

1.3. Вступление в силу документа

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

1.3.2. Все изменения и дополнения в настоящее Положение вносятся приказом генерального директора Общества.

2. ПОНЯТИЯ И ТЕРМИНЫ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ПОЛОЖЕНИИ

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

- автоматизированная система защиты от утечек информации (система) – система для контроля и управления инцидентами информационной безопасности, контроля за использованием и предупреждения разглашения или неправомерного использования конфиденциальной информации в информационных системах, а также мониторинга трудовой деятельности и анализа работы сотрудников Общества, защиты их законных прав и интересов, бережного отношения к имуществу Общества, соблюдения правил внутреннего трудового распорядка, поддержания трудовой дисциплины;

- 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;

- 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;
- **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;
- **информационно-коммуникационная инфраструктура Общества** - совокупность технических и программных средств, коммуникаций, технологий, стандартов и протоколов, принадлежащих Обществу и обеспечивающих создание, передачу, обработку, использование, хранение, защиту и уничтожение информации, обрабатываемой в Обществе;
- **автоматизированное рабочее место (АРМ)** – совокупность компьютерного оборудования, программного обеспечения и информационных ресурсов, предоставленная сотруднику Общества для выполнения им своих должностных обязанностей;
- **средства обработки информации** - совокупность технических, программных и организационных ресурсов, используемых для сбора, хранения, преобразования, передачи и представления информации. К ним относятся как отдельные устройства (АРМ), так и системы, состоящие из нескольких компонентов, а также программное обеспечение и методы организации работы с информацией;
- **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.

2.2. Для обозначения обязательности выполнения требований в Положении применяются понятия «должен», «необходимо» и производные от них. Требования обязательности не распространяются на правовую самостоятельность органов управления АО «Облкоммунэнерго» при принятии ими решений в рамках их компетенции в соответствии с действующим законодательством и уставом АО «Облкоммунэнерго».

Понятие «как правило/правила» означает, что данное требование является преобладающим, а отступление от него должно быть обосновано.

Понятие «допускается» означает, что данное требование или решение применяется в виде исключения, как вынужденное при соответствующем обосновании.

Понятие «рекомендуется» означает, что данное решение является приоритетным, но не обязательным.

3. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ РАБОТ ПО ЭКСПЛУАТАЦИИ И ОБЕСПЕЧЕНИЮ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ В ОБЩЕСТВЕ

3.1. Организационные положения по обеспечению эксплуатации системы

3.1.1. Средства обработки информации, переданные сотруднику Общества для выполнения своих должностных обязанностей, а также созданная с их помощью информация, является собственностью Общества.

3.1.2. Общество, в соответствии с требованиями законодательства РФ, обязано защищать установленными способами свою конфиденциальную информацию, определяя перечень конфиденциальной информации, правила работы с ней и меры защиты.

В соответствии с этим руководство Общества имеет право использовать автоматизированную систему защиты от утечек информации в Обществе.

3.1.3. Автоматизированные рабочие места пользователей локальной информационной сети Общества (далее – АРМ), каналы связи и иное имущество и оборудование, относящееся к информационно-

коммуникационной инфраструктуре Общества может быть использовано сотрудниками Общества только и исключительно в служебных целях.

3.1.4. Сотрудникам Общества запрещается хранить личную информацию на корпоративных ресурсах (АРМ 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.

Это обусловлено тем, что хранение сотрудниками личной информации на корпоративных ресурсах может привести к несанкционированному доступу к ней, разглашению или использованию, что является нарушением прав сотрудников, а Общество являясь оператором персональных данных, обязано обеспечить их безопасность и защиту от несанкционированного доступа.

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 Системой.

3.1.5. Система не предназначена и не может быть использована для идентификации личности.

3.1.6. Система может использоваться для:

- контроля и управления инцидентами информационной безопасности;
- контроля за использованием информационных ресурсов Общества;
- предупреждения разглашения или неправомерного использования конфиденциальной информации;
- защиты информационного обмена на объектах критической информационной инфраструктуры;
- мониторинга трудовой деятельности и анализа работы сотрудников в Обществе;
- защиты законных прав и интересов сотрудников Общества;
- бережного отношения к имуществу Общества;
- соблюдения правил внутреннего трудового распорядка и поддержания трудовой дисциплины в Обществе.

3.1.7. Система проводит мониторинг деятельности сотрудников Общества только на устройствах входящих в информационно-коммуникационную инфраструктуру Общества.

Работа Системы не может производиться и не имеет технической возможности производиться на личных компьютерных устройствах и

оборудовании сотрудников Общества, в том числе и при удаленной работе, а также на устройствах мобильной связи (мобильных телефонах, смартфонах), принадлежащих Обществу, и переданных сотрудникам для выполнения работ в соответствии с должностными инструкциями.

3.1.8. Мониторинг на устройствах входящих в информационно-коммуникационную инфраструктуру Общества является ОТКРЫТЫМ, т.е. Система надлежащим образом размещает на устройствах визуализации АРМ (компьютерных мониторах) специальный значок, сигнализирующий сотруднику Общества о ведении мониторинга Системой на данном устройстве.

3.1.9. Сотрудники Общества должны быть надлежащим образом оповещены об использовании Системы в Обществе путем размещения настоящего Положения и приказа генерального директора Общества о начале действия Системы на информационных ресурсах Общества: сайтах — https://www.oao-oke.ru/ и http://site для беспрепятственного ознакомления всеми сотрудниками Общества.

3.1.10. Все сотрудники Общества использующие, в соответствии со своими должностными обязанностями, устройства входящие в информационно-коммуникационную инфраструктуру Общества и находящиеся под контролем Системы предоставляют на добровольной основе, без принуждения и недопонимания сути свои письменные уведомления об использовании системы защиты от утечек информации (далее – Уведомление). (Приложение №2)

Если у сотрудника Общества существуют мотивированные возражения против порядка применения Системы, он имеет право обратиться с ними к руководству Общества. Возражения сотрудника против порядка применения Системы или отказ подписать Уведомление не отменяют использование Системы на компьютерном оборудовании, принадлежащем Обществу, которое использует сотрудник для осуществления своих должностных обязанностей.

3.1.11 Руководитель структурного подразделения в установленные приказом генерального директора Общества сроки организует ознакомление подчиненных ему сотрудников с настоящим Положением и получение от сотрудников письменных Уведомлений. Подлинники Уведомлений с подписями сотрудников передаются в отдел кадров Общества для хранения в личных делах сотрудников.

3.1.12 Начальник отдела кадров готовит и вносит необходимые для функционирования Системы правовые основания и условия в Коллективный договор Общества, а также в трудовые (гражданско-правовые) договора сотрудников Общества в установленные приказом генерального директора Общества сроки.

3.2. Функции и возможности системы

3.2.1. Возможности Системы предусматривают:

- выявление фактов неправомерной передачи конфиденциальной информации из информационной системы через различные типы сетевых соединений, включая сети связи общего пользования и реагирование на них;
- выявление фактов неправомерной записи конфиденциальной информации на съемные носители информации и реагирование на них;
- фиксирование вывода на печать документов, содержащих конфиденциальной информацию;
- выявление фактов неправомерного копирования конфиденциальной информации из буфера обмена и реагирование на них;
- контроль хранения конфиденциальной информации на серверах и автоматизированных рабочих местах;
- выявление фактов хранения конфиденциальной информации на общих сетевых ресурсах (общие папки, системы документооборота, базы данных, почтовые архивы и иные ресурсы).

3.2.2. Система фиксирует все факты отправки / получения информации по любым каналам, доступным компьютеру, планшету и другим устройствам, входящим в информационно-коммуникационную сеть Общества. В системе сохраняется время отправки, тип устройства, логин пользователя, канал отправки, также сохраняются теневые копии отправленных файлов и информация, содержащаяся в теле письма. Также фиксируются тексты сообщений в мессенджерах. Эти данные имеют юридическую силу, при условии уведомления сотрудников о работе на АРМ автоматизированной системы защиты от утечек информации.

3.2.3. Система производит в рабочее время сотрудников Общества контроль, учет и анализ действий пользователей и администраторов информационно-коммуникационной сети Общества (в соответствии со ст.22 ТК РФ о праве работодателя проводить самостоятельно оценку соблюдения требований трудового законодательства).

Система автоматически собирает с компьютеров сотрудников информацию об их деятельности на рабочем месте, с учетом функционала сотрудника, анализирует эти данные и создает отчеты о продолжительности и эффективности использования рабочего времени. Система позволяет контролировать начало и конец рабочего дня, отслеживать время, которое затрачивает сотрудник при выполнении определенных задач, а также анализировать использование приложений и интернет-ресурсов в рабочее время, определяя уровень продуктивности сотрудника.

Система позволяет руководителю Общества эффективно распределять ресурсы и оптимизировать рабочие процессы.

3.2.4 В случае выявления Системой нарушений сотрудниками Общества правил внутреннего трудового распорядка, правил обработки конфиденциальной информации, нарушений требований настоящего

Положения и иных инцидентов руководство Общества имеет право назначить служебное расследование в отношении данного сотрудника.

3.3. Организация работ по эксплуатации и обслуживанию Системы

3.3.1. В целях организации работ по эксплуатации и обслуживанию Системы в Обществе приказом генерального директора Общества назначаются:

– уполномоченное лицо,

– структурное подразделение ответственное за эксплуатацию и обслуживание Системы.

3.3.2. Указанные лица и подразделения отвечают за проведение следующих мероприятий:

Уполномоченное лицо за:

– определение и описание перечня конфиденциальной информации;

– разработку регламентов и положений и внедрение соответствующих организационных мер;

Структурное подразделение за:

- поддержание в актуальном состоянии организационно-распорядительной документации, относящейся и/или регулирующий эксплуатацию Системы;

– обеспечение непрерывного и устойчивого функционирования Системы;

– формирование сотрудниками структурного подразделения, ответственного за эксплуатацию и обслуживание Системы отчетов и справок по запросу уполномоченного лица на основе информации, содержащейся в Системе;

– анализ, на основе информации содержащейся в Системе, возможных каналов и способов утечек информации и проведение мероприятий по их устранению, включающие организационные, физические и технические меры и средства защиты;

– закупку, установку и настройку технических средств защиты информации;

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

3.3.3. Сотрудников структурного подразделения, ответственного за эксплуатацию и обслуживание Системы, назначает для выполнения конкретных задач и определяет их функции уполномоченное лицо.

3.3.4. Сотрудники, ответственные за эксплуатацию и обслуживание Системы, перед допуском к работам должны подписать Обязательство, о неразглашении конфиденциальной информации, не содержащей сведений, составляющих государственную тайну (Приложение №4).

3.4. Контроль работ по эксплуатации и обслуживанию системы

3.4.1. Контроль работ по эксплуатации и обслуживанию Системы в Обществе (далее – контроль, контрольные мероприятия) осуществляется путем проведения анализа, содержащийся в системе информации, периодических плановых внутренних контрольных мероприятий и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

3.4.2. В рамках проведения контрольных мероприятий выполняются:

– проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению защиты от утечек информации;

– проверка осведомленности и соблюдения сотрудниками структурного подразделения, ответственного за эксплуатацию и обслуживание системы, требований к обеспечению защиты от утечек информации;

– проверка соответствия перечня сотрудников Общества, которым предоставлен доступ к конфиденциальной информации (Персональные данные);

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

– инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению защиты от утечек информации (при необходимости);

– проверка соответствия организационно-распорядительной документации по обеспечению защиты от утечек информации действующим требованиям законодательства РФ, руководящих документов ФСБ России, ФСТЭК России.

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

3.4.4. Плановые контрольные мероприятия проводятся как периодически в соответствии с планом проведения мероприятий по осуществлению внутреннего контроля, так и по решению уполномоченного лица, а также в случае возникновения инцидентов информационной безопасности.

3.4.5. Внеплановые проверки в Обществе в обязательном порядке проводятся в случае выявления следующих фактов:

–нарушение конфиденциальности, целостности, доступности конфиденциальной информации;

– халатность и несоблюдение требований к обеспечению безопасности конфиденциальной информации;

– нарушение условий хранения носителей конфиденциальной информации;

– использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) конфиденциальной информации или другим нарушениям, приводящим к снижению уровня защищенности конфиденциальной информации.

3.4.6. 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.

3.5. Совершенствование системы

3.5.1. Ежегодно структурное подразделение ответственное за эксплуатацию Системы направляет уполномоченному лицу отчет о проделанных мероприятиях по обеспечению защиты информации в Обществе.

3.5.2. Необходимость реализации мероприятий по обеспечению защиты от утечек информации в Обществе может быть обусловлена:

– результатами проведенных контрольных мероприятий;

– изменениями федерального законодательства в области защиты информации;

– изменениями структуры процессов защиты информации в Обществе;

– результатами анализа инцидентов информационной безопасности;

– результатами мероприятий по контролю и надзору за обработкой конфиденциальной информации, проводимых уполномоченным органом;

– жалоб и запросов субъектов персональных данных.

3.5.3. На основании решения, принятого уполномоченным лицом по результатам рассмотрения ежегодного отчета, в структурном подразделении, ответственном за эксплуатацию Системы составляется план работ по обеспечению безопасности информации в Обществе на следующий год.

Приложение №1

к Положению о порядке эксплуатации
автоматизированной системы защиты
от утечек информации в
АО «Облкоммунэнерго»

Перечень должностей сотрудников АО «Облкоммунэнерго», на рабочих местах которых предусматривается использование автоматизированной системы защиты от утечек информации

Перечень должностей сотрудников Общества, на рабочих местах которых предусматривается использование модулей Системы – мониторинг трудовой деятельности и анализ работы сотрудников + контроль утечек информации
Отдел координации закупок
Ведущий инженер материально-технического обеспечения
Специалист по закупкам и договорным отношениям
Отдел кадров
Начальник отдела
Специалист по кадрам
Специалист по работе с персоналом
Отдел по организационной работе и связям с общественностью
Секретарь генерального директора
Архивист
Специалист по организационной работе
Специалист по делопроизводству
Служба охраны труда, промышленной безопасности, ГО и ЧС
Заместитель начальника службы
Специалист по охране труда 1 категории
Отдел информационных технологий, телекоммуникаций и связи
Заместитель начальника отдела
Ведущий инженер-программист
Ведущий инженер-программист
Ведущий инженер-программист
Инженер-программист
Инженер
Специалист по информационной безопасности

Инженер - программист
Центральная бухгалтерия
Заместитель главного бухгалтера
Ведущий бухгалтер по учету затрат филиалов
Ведущий бухгалтер по расчетам с подотчетными лицами
Ведущий бухгалтер по хозяйственным операция и расчетам с поставщиками
Ведущий бухгалтер по расчету заработной платы
Ведущий бухгалтер по расчетам с покупателями и формированию НДС
Ведущий бухгалтер по ведению кассовых операций и расчету заработной платы
Бухгалтер по расчету заработной платы
Отдел баланса электроэнергии
Заместитель начальника отдела
Ведущий инженер
Ведущий инженер по расчетам и режимам организации электроэнергетики
Инженер по расчетам
Финансово-экономический отдел
Начальник финансово-экономического отдела
Заместитель начальника отдела
Ведущий экономист
Ведущий экономист по труду
Ведущий экономист
Административно–хозяйственный отдел
Начальник отдела
Специалист по производственно-техническим вопросам
Служба главного метролога
Заместитель главного метролога
Ведущий инженер по метрологии
Главный метролог
Инженер по метрологии службы главного метролога
Инженер по обслуж. АСКУЭ
ведущий инженер по обслуживанию АСКУЭ
Отдел технологического присоединения
Ведущий инженер
Инженер
Инженер по технологическому присоединению
Инженер
Инженер ОТП
Группа по прочей деятельности
Начальник отдела изысканий

Ведущий инженер-проектировщик
Ведущий инженер
Ведущий инженер
Ведущий инженер-проектировщик
Ведущий инженер по работе с проектно-сметной документацией
Ведущий экономист
Ведущий инженер
Производственно-технический отдел
Заместитель начальника отдела
Ведущий инженер
Ведущий специалист ПТО
Ведущий инженер по техническому ремонту и эксплуатации электросетей
Юридическая служба
Заместитель начальника службы
Ведущий юрисконсульт
Ведущий юрисконсульт
Ведущий юрисконсульт
Юрисконсульт
Служба релейной защиты, автоматики и электротехнической лаборатории
Начальник службы
Заместитель начальника службы
Ведущий инженер
Ведущий инженер
Ведущий инженер
Ведущий инженер
Отдел механизации и транспорта
Главный механик

Перечень должностей сотрудников Общества, на рабочих местах которых предусматривается использование модуля Системы – контроль утечек информации
Отдел координации закупок
Ведущий специалист по закупкам и договорным отношениям
Специалист по закупкам и договорным отношениям
Служба охраны труда, промышленной безопасности, ГО и ЧС
Ведущий специалист по ПБ
Центральная бухгалтерия
Ведущий бухгалтер по банковским операциям

Финансово-экономический отдел
Заместитель начальника отдела
Группа по прочей деятельности
Ведущий экономист

Приложение №2

к Положению о порядке эксплуатации
автоматизированной системы защиты
от утечек информации в
АО «Облкоммунэнерго»

Уведомление сотрудника АО «Облкоммунэнерго» об использовании системы защиты от утечек информации

Я, _____
(Фамилия, имя, отчество)
исполняющий(ая) должностные обязанности по занимаемой должности
_____
(должность, наименование структурного подразделения)
конкретно, предметно, без недопонимания сути, проинформирован, что на компьютерных устройствах входящих в информационно-коммуникационную инфраструктуру АО «Облкоммунэнерго» (далее – Общество) используется автоматизированная система защиты от утечек информации (далее – Система). Внедрение и эксплуатация Системы основано и соответствует действующему законодательству РФ и внутренним нормативно-правовым актам Общества.

Я надлежащим образом проинформирован(а), что:

1. Средства обработки информации, переданные сотруднику Общества для выполнения своих должностных обязанностей, а также созданная с их помощью информация, является собственностью Общества.

2. Общество, в соответствии с требованиями законодательства РФ, обязано защищать установленными способами свою конфиденциальную информацию, определяя перечень конфиденциальной информации, правила работы с ней и меры защиты.

В соответствии с этим руководство Общества имеет право использовать автоматизированную систему защиты от утечек информации в Обществе.

3. Автоматизированные рабочие места пользователей локальной информационной сети Общества (далее – АРМ), каналы связи и иное имущество и оборудование, относящееся к информационно-коммуникационной инфраструктуре Общества может быть использовано сотрудниками Общества только и исключительно в служебных целях.

4. Сотрудникам Общества запрещается хранить личную информацию на корпоративных ресурсах (АРМ 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.

Это обусловлено тем, что хранение сотрудниками личной информации на корпоративных ресурсах может привести к несанкционированному доступу к ней, разглашению или использованию, что является нарушением прав сотрудников, а Общество являясь оператором персональных данных, обязано обеспечить их безопасность и защиту от несанкционированного доступа.

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 Системой.

5. Система не предназначена и не может быть использована для идентификации личности.

6. Система может 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,
- 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.

7. Система проводит мониторинг деятельности сотрудников Общества только на устройствах входящих в информационно-коммуникационную инфраструктуру Общества.

Работа Системы не может производиться и не имеет технической возможности производиться на личных компьютерных устройствах и устройствах мобильной связи сотрудников Общества, в том числе и при удаленной работе. Работа Системы не может производится на устройствах мобильной связи (мобильных телефонах, смартфонах), принадлежащих Обществу, и переданных сотрудникам для выполнения работ в соответствии с должностными инструкциями.

8. Мониторинг на устройствах входящих в информационно-коммуникационную инфраструктуру Общества является ОТКРЫТЫМ, т.е. Система надлежащим образом размещает на устройствах визуализации АРМ

(компьютерных мониторах) специальный значок, сигнализирующий сотруднику Общества о ведении мониторинга Системой на данном устройстве.

9. Я проинформирован(а), что если у меня существуют мотивированные возражения против порядка применения Системы в Обществе, то я имею право обратиться с ними к руководству Общества.

10. Я проинформирован(а), что мои возражения против порядка применения Системы или отказ подписать настоящее Уведомление не отменяют использование Системы на компьютерном оборудовании, принадлежащем Обществу, с использованием которого сотрудник Общества осуществляет свои должностные обязанности.

_____ /_____/
(подпись) (расшифровка)

Дата подписания «_____» _____20____ г.

Приложение №3

к Положению о порядке эксплуатации
автоматизированной системы защиты
от утечек информации в
АО «Облкоммунэнерго»

Текст для внесения дополнений в Коллективный договор АО «Облкоммунэнерго», а также в трудовые (гражданско-правовые) договора сотрудников Общества путем заключения дополнительных соглашений.

В соответствии со ст.56 ТК РФ руководство Общества для контроля исполнения должностных обязанностей сотрудниками Общества имеет право использовать системы автоматизированного контроля.

В качестве систем автоматизированного контроля в Обществе могут использоваться системы видеонаблюдения, системы контроля и управления доступом а также DLP-системы - специализированное программное обеспечение, предназначенное для контроля исполнения должностных обязанностей сотрудниками Общества и защиты от утечек конфиденциальной информации.

Приложение №4

к Положению о порядке эксплуатации
автоматизированной системы защиты
от утечек информации в
АО «Облкоммунэнерго»

Обязательство, о неразглашении конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

Я, _____
(Фамилия, имя, отчество)
исполняющий(ая) должностные обязанности по занимаемой должности
_____
(должность, наименование структурного подразделения)
предупрежден(а), что на период исполнения должностных обязанностей по эксплуатации автоматизированной системы защиты от утечек информации, в соответствии с Положением о порядке эксплуатации системы, мне будет предоставлен допуск к конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

Настоящим добровольно, без недопонимания сути, принимаю на себя следующие обязательства:

1. Строго соблюдать законодательство Российской Федерации и внутренние нормативные документы Общества, регламентирующие порядок и правила работы с конфиденциальной информацией и персональными данными.
2. Учитывать, что вся информация, подготовленная (созданная) при использовании информационных, технических или других ресурсов Общества, являются собственностью Общества.
3. Не передавать и не раскрывать третьим лицам конфиденциальную информацию, которая мне доверена (будет доверена) или станет известной в связи с выполнением должностных обязанностей без письменного распоряжения на выполнение таких действий руководителя Общества и/или руководителя структурного подразделения, в котором я непосредственно работаю.
4. В случае попытки третьих лиц получить от меня конфиденциальную информацию, немедленно сообщать об этом непосредственному руководителю.
5. Не использовать конфиденциальную информацию с целью получения личной выгоды.
6. В случае моего увольнения, все носители конфиденциальной информации (черновики, таблицы, магнитные и оптические носители,

дискеты, flash-накопители, распечатки на принтерах, и пр.), которые находились в моём распоряжении в связи с выполнением мною служебных обязанностей во время работы в Обществе, передать лично руководителю Общества или руководителю структурного подразделения, в котором я непосредственно работал(а).

7. Об утрате носителей информации, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), и о других фактах, которые могут привести к нарушению правил обработки информации немедленно сообщать специалисту по информационной безопасности или лично руководителю Общества.

8. Немедленно доводить до сведения руководства известные мне факты разглашения или создания предпосылок к разглашению конфиденциальной информации.

9. В течение года после прекращения права на допуск к конфиденциальной информации не разглашать и не передавать третьим лицам известную мне конфиденциальную информацию, связанную с работой в Обществе.

Я, на период моей работы в Обществе, предоставляю руководству Общества право при необходимости проверять соблюдение мной требований Положения о порядке эксплуатации автоматизированной системы защиты от утечек информации в Обществе и иных требований безопасности методами, разрешенными законами Российской Федерации.

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» и «Положением о порядке эксплуатации автоматизированной системы защиты от утечек информации в АО «Облкоммунэнерго».

Обязательство исполняется в двух экземплярах. После подписания один экземпляр обязательства вручается сотруднику, второй хранится в его личном деле.

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

_____ / _____ /
(подпись) (расшифровка)

Дата подписания «_____» _____ 20____ г.

Лист согласования

Внутренний документ "Об утверждении положения «О порядке эксплуатации автоматизированной системы защиты от утечек информацией в АО «Облкоммунэнерго»"

Должность	ФИО	Результат	Дата	Комментарий
Заместитель генерального директора по перспективному развитию	Хаметов Ренат Хафисович	Согласовано	02.07.2025	
Начальник отдела по организационной работе и связям с общественностью	Сошественская Ольга Михайловна	Согласовано	30.06.2025	
Начальник отдела кадров	Худошина Оксана Александровна	Согласовано	02.07.2025	
Главный инженер	Качалов Александр Федорович	Согласовано	02.07.2025	
Начальник отдела информационных технологий, телекоммуникаций и связи	Пономаренко Антон Сергеевич	Согласовано	30.06.2025	
Начальник юридической службы	Тимощенко Сергей Владимирович	Согласовано	02.07.2025	