РЕГИОНАЛЬНАЯ ЭНЕРГЕТИЧЕСКАЯ КОМИССИЯ ОМСКОЙ ОБЛАСТИ

П Р И К А З

17 мая 2013 года № 5-17

г. Омск

Об утверждении положения об обработке и обеспечении безопасности персональных данных в Региональной энергетической комиссии Омской области

Во исполнение Федерального закона «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» приказываю:

1. Утвердить положение об обработке и обеспечении безопасности персональных данных в Региональной энергетической комиссии Омской области (далее - РЭК Омской области) согласно приложению к настоящему приказу.

2. Контроль за выполнением настоящего приказа возложить на заместителя председателя РЭК Омской области А.Ю. Меньшикова.

Председатель
Региональной энергетической
комиссии Омской области Д.А. Русских

Приложение
к приказу Региональной
энергетической комиссии Омской области
от 17 мая 2023 года № 5-17

ПОЛОЖЕНИЕ
об обработке и обеспечении безопасности персональных данных в Региональной энергетической комиссии Омской области

Термины, определения и сокращения

Персональные данные – любая информация, относящаяся к прямо или косвенно, определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор (персональных данных) – Региональная энергетическая комиссия Омской области (далее - РЭК Омской области) организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых оператором с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств автоматизации оператора.

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

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

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

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

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

Информационная система персональных данных – совокупность содержащихся в базах данных оператора персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

ИС – информационная система.

ИСПДн – информационная система персональных данных.

ПДн – персональные данные.

АРМ – автоматизированное рабочее место.

ПЭВМ – персональная электронно-вычислительная машина.

НСД – несанкционированный доступ.

СЗИ – средство защиты информации.

1. Общие положения

1.1. Положение об обработке и обеспечении безопасности персональных данных (далее – Положение) в РЭК Омской области разработаны на основании требований, установленных:

Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – № 152-ФЗ);

Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Нормативными методическими документами Федеральной службы по техническому и экспертному контролю Российской Федерации по обеспечению безопасности ПДн при их обработке в ИСПДн.

1.2. Настоящее Положение вступает в силу с момента его утверждения председателем РЭК Омской области и действует бессрочно, до замены его новым Положением.

1.3. Все изменения и дополнения в Положение вносятся соответствующими приказами РЭК Омской области.

1.4. Целью настоящего Положения является организация обработки и обеспечения защиты ПДн граждан от НСД, неправомерного их использования, модификации или их утраты.

1.5. Общее руководство осуществляет председатель РЭК Омской области в организации работ по обработке и обеспечении безопасности ПДн в РЭК Омской области.

2. Перечень обрабатываемых Пдн

2.1. В РЭК Омской области обрабатываются следующие ПДн:

– о сотрудниках организации (фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения), число, месяц, год рождения, место рождения, информация о гражданстве (в

том числе предыдущие гражданства, иные гражданства), вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи, адрес места жительства (адрес регистрации, фактического проживания), номер контактного телефона или сведения о других способах связи, реквизиты страхового свидетельства государственного пенсионного страхования, идентификационный номер налогоплательщика, реквизиты страхового медицинского полиса обязательного медицинского страхования, реквизиты свидетельства государственной регистрации актов гражданского состояния, семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших), сведения о трудовой деятельности, сведения о воинском учете и реквизиты документов воинского учета, сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании), сведения об ученой степени, информация о владении иностранными языками, степень владения, фотография, сведения о прохождении государственной гражданской службы, информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту, сведения о пребывании за границей, информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы, информация о наличии или отсутствии судимости, информация об оформленных допусках к государственной тайне, государственные награды, иные награды и знаки отличия, сведения о профессиональной переподготовке и (или) повышении квалификации, информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания, сведения о доходах, об имуществе и обязательствах имущественного характера, номер расчетного счета, номер банковской карты);

3. Категория субъектов

3.1. К субъектам ПДн относятся:

– сотрудники РЭК Омской области;

3.2. К субъектам, которые обрабатывают ПДн, относятся:

– администратор – сотрудник РЭК Омской области, ответственный за настройку, внедрение, предоставление и разграничение доступа конечного пользователя (оператора АРМ) к элементам, хранящим персональные данные.

– оператор (пользователь) АРМ – сотрудник РЭК Омской области, осуществляющий обработку ПДн. Обработка ПДн включает: сбор, запись, хранение, уточнение, обезличивание, удаление, уничтожение. Оператор не имеет полномочий для управления подсистемами обработки данных.

4. Условия и порядок обработки ПДн

4.1. Администратор и операторы участвующие в обработке ПДн назначаются распоряжением председателя РЭК Омской области.

4.2. Сотрудники, допущенные к обработке ПДн, должны быть ознакомлены под расписку с документами, устанавливающими порядок обработки ПДн. С данными сотрудниками проводится инструктаж по порядку обработки ПДн и способах их защиты. Данный факт отражается в журнале инструктажа пользователей и ответственных лиц ИСПДн (приложение № 5 к Положению).

4.3. Сотрудники РЭК Омской области, допущенные к обработке ПДн, в случае освобождения их от замещаемой должности и (или) увольнения обязаны прекратить обработку ПДн, ставших известными им в связи с исполнением должностных обязанностей, в соответствии с заключенным Обязательством о неразглашении информации, содержащей персональные данные (приложение № 1 к Положению).

4.4. Обработка ПДн может осуществляться только с согласия субъектов ПДн. Согласие на обработку ПДн может быть дано представителем субъекта ПДн.

4.5. Письменное согласие субъекта ПДн на обработку своих ПДн должно включать в себя:

- Фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе.
- Цель обработки ПДн.
- Перечень ПДн, на обработку которых дается согласие субъекта ПДн.
- Перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых способов обработки ПДн.
- Срок, в течение которого действует согласие, а также порядок его отзыва.
- Подпись субъекта ПДн.

4.6. Форма согласия субъекта ПДн на обработку своих ПДн оформляется в виде анкеты (приложение № 2 к Положению).

4.7. Согласие на обработку ПДн может быть отозвано субъектом ПДн в любое время на основании его личного заявления, поданного на имя Председателя.

4.8. РЭК Омской области обеспечивает конфиденциальность обрабатываемых ПДн субъектов ПДн.

4.9. В отношении ПДн субъектов вводится режим ограничения доступа. Список должностных лиц, имеющих доступ к ПДн, субъекты - только те сотрудники РЭК Омской области, которым ПДн необходимы в связи с исполнением ими должностных обязанностей, утверждаются Председателем РЭК Омской области.

4.10. Обработка ПДн осуществляется на аттестованном под обработку ПДн АРМ.

4.11. Классификация ПДн осуществляется документами ФСТЭК России и в порядке, установленном законодательством Российской Федерации.

4.12. Безопасность ПДн, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн.

4.13. Доступ пользователей к ПДн в информационных системах ПДн разрешается после обязательного прохождения процедуры идентификации и аутентификации. Сотрудникам РЭК Омской области, имеющим право осуществлять обработку ПДн предоставляется уникальный логин и пароль для доступа к информационной системе.

4.14. При эксплуатации автоматизированной системы необходимо соблюдать требования:

4.15. к работе допускаются только назначенные лица;

4.16. на ПЭВМ на которых обрабатываются и хранятся сведения о ПДн, должны быть установлены пароли (идентификаторы);

4.17. на период обработки защищаемой информации в помещении могут находиться лица, допущенные в установленном порядке к обрабатываемой информации.

4.18. Не допускается обработка ПДн в ИС с использованием средств автоматизации при отсутствии:

1) утвержденных организационно-технических документов о порядке эксплуатации ИСПДн;

2) настроенных средств защиты информации в соответствии с требованиями безопасности информации;

3) охраны и организации режима допуска в помещения, предназначенные для обработки ПДн.

4.19. Передача ПДн осуществляется только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

4.20. Сроки обработки и хранения ПДн определяются:

1) достижением цели обработки ПДн;

2) иными требованиями законодательства Российской Федерации и ведомственными нормативно-правовыми актами.

4.21. Хранение ПДн осуществляется в кабинетах № 308, 322 РЭК Омской области.

4.22. Безопасность при хранении ПДн субъектов ПДн обеспечивается с помощью системы защиты ПДн, включающей организационные меры и СЗИ.

4.23. Помещения, в которых производится обработка и (или) хранение сведений, содержащих ПДн, при отсутствии в нём сотрудников РЭК Омской области должно быть закрыто, а компьютеры должны быть выключены или заблокированы.

4.24. Проведение уборки помещения, в котором хранятся ПДн, должно производиться в присутствии сотрудников РЭК Омской области.

4.25. Сотрудники, производящие обработку ПДн обязаны:

1) соблюдать требования, обеспечивающие сохранность документов, их защиту от вредных воздействий окружающей среды (пыли, воздействия солнечного тепла), механических и иных повреждений;

2) соблюдать порядок работы с документами и базами данных, содержащими ПДн;

3) не оставлять документы на рабочих местах в раскрытом виде и без присмотра.

4.26. Лица, ответственные за организацию обработки ПДн, ответственные за обеспечение безопасности ПДн при их обработке в ИСПДн, должны обеспечить:

1) своевременное обнаружение фактов НСД к ПДн и немедленное доведение этой информации до ответственных лиц и председателя РЭК Омской области;

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

3) возможность восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;

4) постоянный контроль за обеспечением уровня защищенности ПДн;

5) знание и соблюдение условий использования СЗИ, предусмотренных эксплуатационной и технической документацией;

6) учет применяемых СЗИ, эксплуатационной и технической документации к ним, носителей ПДн;

7) при обнаружении нарушений порядка предоставления ПДн незамедлительное приостановление предоставления ПДн пользователям ИСПДн до выявления причин нарушений и устранения этих причин;

8) разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей ПДн, использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к

снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

4.27. Администратор, ответственный за обеспечение функционирования ИСПДн, принимает все необходимые меры по восстановлению ПДн, модифицированных или удаленных, уничтоженных вследствие НСД к ним.

4.28. В случае выявления нарушений порядка обработки ПДн в информационных системах ПДн уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

5. Порядок учета, обращения и уничтожения машинных носителей информации

5.1. В РЭК Омской области ведется учёт машинных носителей информации, содержащей ПДн.

5.2. В процессе первоначального учёта составляется перечень имеющихся машинных носителей ПДн с указанием состава имеющихся на них ПДн.

5.3. Каждому носителю ПДн присваивается учётный номер.

5.4. На съемные носители, на которые наклеивание ярлыка недопустимо по техническим причинам, реквизиты ярлыка полностью наносятся на диск специальным нестираемым маркером.

5.5. После присвоения учётного номера осуществляется регистрация носителя в Журнале учёта машинных носителей информации (приложение № 3 к Положению).

5.6. Ведение Журнала возлагается на назначенного сотрудника.

5.7. При использовании машинных носителей ПДн запрещается:

– использовать неучтенные машинные носители;

– хранить машинные носители с ПДн вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

– выносить машинные носители с ПДн из кабинетов для работы с ними вне помещений РЭК Омской области.

5.8. При утрате или уничтожении машинного носителя персональных данных немедленно ставится в известность председатель РЭК Омской области. На утраченные носители составляется акт. Соответствующие отметки вносятся в Журнал учета машинных носителей информации (приложение № 3 к Положению).

5.9. Машинные носители информации, содержащие ПДн, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с ПДн осуществляется комиссионно. Уничтожение ПДн на машинных носителях производится

путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление ПДн, или удалением методами и средствами гарантированного удаления остаточной информации. Уничтожение машинных и материальных носителей ПДн производится комиссионно с составлением соответствующего акта (приложение № 4 к Положению).

5.10. Под уничтожением обработанных ПДн понимаются действия, в результате которых невозможно восстановить содержание ПДн в ИСПДн или в результате которых уничтожаются машинные и материальные носители ПДн.

6. Процедуры, направленные на выявление и предотвращение нарушений законодательства в сфере ПДн

6.1. Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты ПДн, включающей организационные меры и СЗИ, средства предотвращения НСД, утечки информации по техническим каналам, а также используемые в информационной системе информационные технологии.

6.2. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

6.3. К мерам, направленным на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки ПДн относятся:

– назначение ответственного за организацию обработки ПДн;

– применение правовых, организационных и технических мер по обеспечению безопасности ПДн в соответствии с частями 1 и 2 статьи 19 № 152-ФЗ;

– осуществление внутреннего контроля соответствия обработки ПДн № 152-ФЗ и принятым в соответствии с ним нормативными правовыми актами, требованиям к защите ПДн, политике оператора в отношении обработки ПДн, локальным актам оператора;

– оценка вреда, который может быть причинён субъектам ПДн в случае нарушения законодательства Российской Федерации и настоящего Положения;

– ознакомление сотрудников, непосредственно осуществляющих обработку ПДн с положениями законодательства Российской Федерации о ПДн и настоящим Положением;

– запрет на обработку ПДн лицами, не допущенными к их обработке.

7. Мероприятия по защите ПДн

7.1. Под угрозой или опасностью утраты ПДн понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

7.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

7.3. Защита ПДн представляет собой жестко регламентированный и динамически-технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности ПДн и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности.

7.4. Защиту ПДн от неправомерного их использования или утраты необходимо обеспечивать в порядке, установленном федеральными законами и организационно-распорядительными документами РЭК Омской области в области защиты информации.

7.5. Основным виновником НСД к ПДн является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами.

7.6. Для обеспечения внутренней защиты ПДн необходимо соблюдать ряд мер:

– ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;

– строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

– рациональное размещение рабочих мест сотрудников, исключающее бесконтрольное использование защищаемой информации;

– знание сотрудником требований нормативно-методических документов по защите информации и сохранении тайны;

– наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

– организация хранения персональных данных на материальных носителях;

– определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

– организация порядка уничтожения информации;

– организация и контроль парольной защиты доступа пользователей к информационной системе ПДн;

– применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации;

– своевременное выявление нарушения требований разрешительной системы доступа сотрудников;

– воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты сведений при работе с ПДн.

7.7. Для защиты ПДн создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить НСД и овладение информацией. Целью и результатом НСД к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания документа и др.

7.8. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности РЭК Омской области, посетители, сотрудники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов, содержащих ПДн.

7.9. Для обеспечения внешней защиты ПДн необходимо соблюдать ряд мер:

– соблюдение порядка приема, учёта и контроля деятельности посетителей;

– использование технических средств охраны, сигнализации;

– организация охраны помещений;

– выполнение требований к защите информации при интервьюировании и собеседованиях.

7.10. Все лица, связанные с получением, обработкой и защитой ПДн, обязаны не разглашать полученные ПДн, ставшие ему известные в ходе выполнения им служебных обязанностей.

8. Правила работы с обезличенными данными

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

8.2. Обезличивание ПДн может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых ПДн, снижения класса используемых информационных систем ПДн и по

достижению сроков обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законодательством Российской Федерации.

8.3. К способам обезличивания ПДн в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня ПДн.

8.4. К способам обезличивания ПДн при условии дальнейшей обработки ПДн относятся:

– уменьшение перечня обрабатываемых сведений;
– замена части сведений идентификаторами;
– обобщение (понижение) точности некоторых сведений;
– деление сведений на части и обработка их в разных информационных системах;
– другие способы.

8.5. Обезличенные ПДн не подлежат разглашению и нарушению конфиденциальности.

8.6. Обезличенные ПДн могут обрабатываться с использования и без использования средств автоматизации.

8.7. При обработке обезличенных ПДн с использованием средств автоматизации необходимо:

– использование паролей;
– использование антивирусных программ;
– правил работы со съемными носителями (если они используется);
– правил резервного копирования;
– соблюдение правил доступа в помещение, в котором ведётся обработка ПДн.

8.8. При обработке обезличенных ПДн без использования средств автоматизации необходимо соблюдение:

– хранения бумажных носителей в условиях, исключающих доступ к ним посторонних лиц;
– соблюдение правил доступа в помещение, в котором ведётся обработка ПДн.

8.9. Непосредственно выполнение мероприятий по обезличиванию ПДн с применением того или иного способа обезличивания возлагается на служащих, допущенных к обработке ПДн на основании списка, утвержденного председателем РЭК Омской области, во взаимодействии с лицом, ответственным за организацию обработки ПДн.

9. Правила организации парольной защиты

9.1 Аутентификация авторизированных субъектов доступа осуществляется с помощью парольной защиты (логин + пароль).

9.2 Идентификация осуществляется с помощью средств защита на основе алгоритмов шифрования, электронной подписи и защиты от НСД.

9.3 Личные пароли должны генерироваться с учетом следующих требований:

– длина пароля должна быть не менее 8 символов;

– алфавит пароля не менее 60 символов;

– в числе символов пароля могут присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированного рабочего места и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

9.4. Пользователь обязан хранить в тайне пароль, код и другие средства доступа к информационным ресурсам.

9.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не более чем через 180 дней или незамедлительно при создании предпосылок к его утрате (хищению) и (или) разглашению.

9.6. Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу) должна производиться администратором немедленно после окончания последнего сеанса работы данного пользователя с системой.

9.7. Повторное использование идентификатора пользователя в течение не менее одного года запрещено.

9.8. При установке и переустановке АРМ производится смена (установка) пароля администратора BIOS ПЭВМ с целью ограничения доступа к изменению параметров загрузки и системных характеристик.

9.9. При окончании срока действия пароля администратор парольной защиты обязан сгенерировать и заменить его на новый, не применявшийся ранее.

9.10. Информация о паролях пользователей является конфиденциальной информацией.

9.11. Информация о персональных кодах, электронных ключах и других средств доступа пользователей к информационному ресурсу является конфиденциальной информацией и разглашению не подлежит, должна содержать защиту от доступа посторонних лиц.

9.12. Если пользователь уверен в правильности ввода названия учетной записи и пароля, но ему не удается войти в систему, пользователь обязан незамедлительно сообщить об этом администратору для получения нового пароля.

9.13. Если пользователь заметит несанкционированное появление, изменение или удаление информации, он должен немедленно сообщить об обнаруженных изменениях администратору.

9.14. Набор личного пароля следует проводить, в отсутствии лиц, которые потенциально могут увидеть процесс набора.

9.15. Запрещается:

– передача личного пароля посторонним лицам, в том числе сотрудникам РЭК Омской области;

– вход в компьютерную сеть с использованием чужих паролей доступа;

– оставлять без присмотра рабочее место с открытой пользовательской сессией.

9.16. В случае утраты надежности (компрометации) личного пароля, либо подозрения о компрометации пароля, пользователь обязан незамедлительно поставить об этом в известность администратора для исключения возможности утечки информации и принятия мер по внеплановой смене личного пароля.

9.17. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора.

9.18. Любые действия пользователей и посторонних лиц нарушающие требования настоящего Положения, категорируемые как значимые нарушения и нарушения, имеющие признаки компьютерного преступления, должны анализироваться через процедуру служебного расследования.

10. Порядок доступа в помещения, в которых ведется обработка ПДн

10.1. В служебных помещениях, занимаемых РЭК Омской области, применяются административные, технические, физические и процедурные меры, направленные для защиты данных от нецелевого использования, НСД, раскрытия, потери, изменения и уничтожения, обрабатываемых ПДн.

10.2. Для помещений, в которых обрабатываются ПДн, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей ПДн и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этом помещении посторонних лиц.

10.3. Нахождение в помещении посторонних лиц, возможно только в сопровождении сотрудника РЭК Омской области.

10.4. Внутренний контроль соблюдения порядка доступа в помещение, в котором ведется обработка ПДн, проводится лицом ответственным за организацию обработки Пдн.

11. Порядок организации и проведения мероприятий внутреннего контроля

11.1. С целью осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям в РЭК Омской области организуются и проводятся мероприятия по внутреннему контролю соблюдения правил обработки ПДн.

11.2. Мероприятия по контролю проводятся лицом, ответственным за организацию обработки ПДн, в соответствии с его должностной инструкцией или комиссией, назначенной для проведения мероприятия по контролю распоряжением председателя РЭК Омской области.

11.3. В проведении мероприятия по контролю в качестве члена комиссии не может принимать участие лицо, прямо или косвенно заинтересованное в ее результатах.

11.4. По итогам каждого мероприятия по контролю лицо, ответственное за организацию обработки ПДн, делает соответствующую запись в журнале учёта проведения мероприятий по контролю соблюдения режима защиты ПДн.

11.5. О результатах мероприятия по контролю в случае выявления нарушения лицо, ответственное за организацию обработки ПДн, докладывает председателю РЭК Омской области докладной запиской с указанием вида нарушения, места, обстоятельств, времени совершения нарушения, а также структурного подразделения (отдела), должности, фамилии, имени и отчества лица, допустившего нарушение, и незамедлительно принимает меры к устранению выявленного нарушения. Об устранении нарушения лицо, ответственное за организацию обработки ПДн, докладывает председателю РЭК Омской области.

11.6. В случае невозможности оперативно устранить выявленное нарушение безопасности ПДн председатель РЭК Омской области утверждает план мероприятий по устранению выявленного нарушения с указанием способов, мер, сроков устранения нарушения и должностных лиц, ответственных за выполнение назначенных мероприятий.

11.7. Журнал учёта мероприятий по контролю соответствия обработки ПДн требованиям к защите ПДн (приложение № 6 к Положению) хранится у лица, ответственного за организацию обработки ПДн.

11.8. Виды мероприятий внутреннего контроля и периодичность их проведения:

– контроль соблюдения требований к защите ПДн в соответствии с требованиями Федерального закона «О персональных данных» - ежегодно;

– контроль соблюдения мер парольной защиты ПДн - ежеквартально;

– контроль соответствия используемого программного обеспечения лицензиям и сертификатам - ежемесячно;

– контроль порядка доступа в помещения, в которых ведется обработка ПДн - ежемесячно;

– контроль за выполнением резервного копирования информации, содержащей ПДн - ежеквартально;

– контроль за сохранностью и использованием СЗИ - ежеквартально;

– контроль сохранности машинных носителей информации, содержащих ПДн - ежемесячно;

– контроль актуальности локальных актов по вопросам защиты ПДн – ежегодно.

12. Ответственность за разглашение ПДн

12.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

12.2. Председатель РЭК Омской области, заместители председателя РЭК Омской области, разрешающие доступ сотрудникам к ПДн, несут персональную ответственность за выданное разрешение.

12.3. Каждый сотрудник РЭК Омской области, получающий для работы документ с ПДн, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

12.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

12.5. За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

12.6. Должностные лица, в обязанность которых входит ведение ПДн, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

12.7. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную

тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений, совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

Приложение № 1
к Положению об обработке
и обеспечении безопасности
персональных данных в Региональной
энергетической комиссии Омской области

ОБЯЗАТЕЛЬСТВО
о неразглашении информации, содержащей персональные данные

Я,_____
_____
_____,
(фамилия, имя, отчество лица, допущенного к обработке персональных данных)

исполняющий (-ая) должностные обязанности по замещаемой должности
_____
_____
_____

предупрежден (-а) о том, что на период исполнения должностных обязанностей мне будет предоставлен допуск к информации, содержащей персональные данные.

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. В случае расторжения договора (контракта) и (или) прекращения права на допуск к информации, содержащей персональные данные, обязуюсь прекратить их обработку, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные. В соответствии со статьей 7 Федерального закона «О персональных данных» я уведомлен (-а) о том, что персональные данные являются конфиденциальной информацией, и я обязан (а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Мне известно, что в соответствии со статьей 81 Трудового кодекса за разглашения охраняемой законом тайны (государственной, коммерческой,

служебной и иной), ставшей известной сотруднику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого сотрудника трудовой договор, может быть, расторгнут по инициативе работодателя.

Я предупрежден (а) о том, что нарушение данного обязательства является основанием привлечения к административной и дисциплинарной ответственности и (или) иной ответственности в соответствии с законодательством Российской Федерации.

Ознакомлен: «___»_____ 20__г. _____

_____

(подпись) (расшифровка подписи)

Приложение № 2
к Положению об обработке
и обеспечении безопасности
персональных данных в Региональной
энергетической комиссии Омской области

СОГЛАСИЕ
работника на обработку персональных данных

Я,_____
_____
_____,
(фамилия, имя, отчество лица, допущенного к обработке персональных данных)

зарегистрированный по адресу:
_____
_____
_____ паспорт серия _____ № _____, выдан
_____
___, код подразделения _____, в соответствии со ст. 9 Федерального закона от 27.07.2006г. № 152-ФЗ «О защите персональных данных» даю согласие на обработку своих персональных данных РЭК Омской области, расположенному по адресу:_____
___,

а именно: совершение действий, предусмотренных п. 3 ст. 3 Федерального закона № 152-ФЗ со всеми данными, которые находятся в распоряжении РЭК Омской области с целью начисления заработной платы, исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование, представления организацией-работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС РФ, сведений в ФСС РФ, предоставлять сведения в банк для оформления банковской карты и перечисления заработной платы на карты, и третьим лицам для оформления полиса ДМС, а также предоставлять сведения в случаях, предусмотренных федеральными законами и иными нормативно-правовыми актами, следующих моих персональных данных:

1. Перечень персональных данных, на обработку которых дается согласие:

– фамилия, имя, отчество (в т. ч. предыдущие);

– паспортные данные или данные документа, удостоверяющего личность;

– дата рождения, место рождения;

– гражданство;

– отношение к воинской обязанности и иные сведения военного билета и приписного удостоверения;

– данные документов о профессиональном образовании, профессиональной переподготовки, повышении квалификации, стажировке;

– данные документов о подтверждении специальных знаний;

– данные документов о присвоении ученой степени, ученого звания, списки научных трудов и изобретений и сведения о наградах и званиях;

– знание иностранных языков;

– семейное положение и данные о составе и членах семьи;

– сведения о социальных льготах, пенсионном обеспечении и страховании;

– данные документов об инвалидности (при наличии);

– данные медицинского заключения (при необходимости);

– стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке;

– должность, квалификационный уровень;

– сведения о заработной плате (доходах), банковских счетах, картах;

– адрес места жительства (по регистрации и фактический), дата регистрации по указанному месту жительства;

– номер телефона (стационарный домашний, мобильный);

– данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории РФ (ИНН);

– данные страхового свидетельства государственного пенсионного страхования;

– данные страхового медицинского полиса обязательного страхования граждан.

2. Перечень действий, на совершение которых дается согласие:

Разрешаю Оператору (организации-работодателю) производить с моими персональными данными действия (операции), определенные статьей 3 Федерального закона от 27.07.2006 №152-ФЗ, а именно: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без их использования (на бумажных носителях).

3. Согласие на передачу персональных данных третьим лицам:

Разрешаю обмен (прием, передачу, обработку) моих персональными данных между Оператором (организацией-работодателем) и третьими лицами в соответствии с заключенными договорами и соглашениями, в целях соблюдения моих законных прав и интересов.

4. Сроки обработки и хранения персональных данных:

Настоящее согласие действует в течение всего срока действия трудового договора, до достижения целей обработки персональных данных или в течение срока хранения информации. Обработка персональных данных, прекращается по истечении семи лет после окончания трудового договора работника.

Согласие на обработку данных (полностью или частично) может быть отозвано субъектом персональных данных на основании его письменного заявления.

Права и обязанности в области защиты персональных данных, ответственность за предоставление ложных сведений о себе мне разъяснены.

Настоящее согласие действует с «____» _____- 20___ г.

_____ / _____ / «_____» _____ 20___ г.
(подпись)

Приложение № 3
к Положению об обработке
и обеспечении безопасности
персональных данных в Региональной
энергетической комиссии Омской области

ЖУРНАЛ
учета машинных носителей информации

Начат: ___»_____20__г.

Завершен: ___»_____20__г.

№ п/п	Регистрационный номер/дата учета	Тип / емкость носителя	Серийный номер	Отметка о постановке на учет (ФИО, подпись, дата)	Расписка в получении (ФИО, подпись, дата)	Отметка о снятии с учета, возврата носителя (ФИО, подпись, дата)	Место хранения носителя	Сведения об уничтожени и носителя / стирании информации
1								
2								
3								

Приложение № 4
к Положению об обработке
и обеспечении безопасности
персональных данных в Региональной
энергетической комиссии Омской области

Акт
об уничтожении персональных данных №___

Комиссия в составе:
Председатель комиссии: _____ / Ф.И.О/
Члены комиссии: _____ / Ф.И.О /
_____ / Ф.И.О /

провела отбор носителей персональных данных_____
и установила, что записанная на них в процессе эксплуатации информация, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего съемных носителей _____
(цифрами и прописью)

После утверждения акта, перечисленные носители сверены с записями в акте и на указанных носителях персональные данные уничтожены путем

_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

После утверждения акта, перечисленные носители сверены с записями в акте и уничтожены путем

_____.
(разрезания, сжигания, механического уничтожения и т.п.)

Уничтоженные носители с книг и журналов учета списаны.

Председатель комиссии: _____ / Ф.И.О/
Члены комиссии: _____ / Ф.И.О /
_____ / Ф.И.О /

Приложение № 5
к Положению об обработке
и обеспечении безопасности
персональных данных в Региональной
энергетической комиссии Омской области

ЖУРНАЛ
инструктажа пользователей и ответственных лиц автоматизированной системы персональных данных

Начат: «___»_____20__г.
Завершен: «___»_____20__г.

№ п/п	Должность инструктируемого	Ф.И.О. инструктируемого	Дата инструктажа	Подпись инструкти-руемого	Подпись, Ф.И.О. ответственного лица

Приложение № 6
к Положению об обработке
и обеспечении безопасности
персональных данных в Региональной
энергетической комиссии Омской области

ЖУРНАЛ
учета мероприятий по контролю обеспечения защиты персональных данных

Начат: «___»_____20__г.

Завершен: «___»_____20__г.

№ п/п	Наименование мероприятия	Дата проведения	ФИО исполнителя	Должность исполнителя	Результат (отчет)
1					
2					
3					
4					

Лист ознакомления

№ п/п	Ф.И.О.	Должность	Подпись	Дата	Примечание
1					
2					
3					