Приложение № 3

УТВЕРЖДЕНА
приказом ЧУ ДПО «МЭИ Юга»
от «09» 03.2022 № 43

РОССЕТИ ЮГ
Межрегиональный энергетический институт

Частное учреждение
дополнительного профессионального образования
«Межрегиональный энергетический институт Юга»

ИНСТРУКЦИЯ
о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

Ростов-на-Дону
2022

1. Общие положения

1.1. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее - Инструкция) содержит обязательные для всех лиц, допущенных к работе с персональными данными в Частном учреждении дополнительного профессионального образования «Межрегиональный энергетический институт Юга» (ЧУ ДПО «МЭИ Юга») (далее - Институт), требования по обеспечению конфиденциальности документов, содержащих персональные данные.

1.2. Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации 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 и другая информация.

1.3. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных или в отношении общедоступных персональных данных.

В общедоступные источники персональных данных (в том числе справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

1.4. Конфиденциальность персональных данных предусматривает обязательное согласие субъекта персональных данных или наличие иного законного основания на их обработку. Согласие субъекта персональных данных не требуется на обработку данных:

- в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;
- адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;
- данных, включающих в себя только фамилии, имена и отчества;
- в целях однократного пропуска на территорию, или в иных аналогичных целях;
- персональных данных, обрабатываемых без использования средств автоматизации.

1.5. В Институте формируется и ведётся перечень конфиденциальных данных, определены места хранения и ответственные за хранение и обработку данных. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, **запрещается.**

2. Нормативные документы, определяющие основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных и использования средств автоматизации

2.1. К нормативным документам, определяющим основные требования и

мероприятия по обеспечению безопасности при обработке и хранении персональных данных и использования средств автоматизации, относятся:

- Конституция Российской Федерации;

- Трудовой кодекс Российской Федерации;

- Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных»;

-Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 года №1119;

- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687.

2.2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

3. Общие правила хранения и передачи персональных данных

3.1. **Запрещается** оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных.

3.2. Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, **запрещается.**

3.3. Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации "О персональных данных", "О порядке рассмотрения обращений граждан Российской Федерации", действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

3.4. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и

обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

4. Ответственность за защиту обрабатываемых персональных данных

Руководители структурных подразделений Института, лица, осуществляющие обработку и хранение конфиденциальных данных в Институте, несут ответственность за обеспечение их информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами.

5. Порядок ознакомления с Инструкцией

Руководители структурных подразделений и лица, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией.

6. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой без использования средств автоматизации

6.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.

6.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

6.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель

не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающее одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

6.5. Использование типовых форм документов и журналов учета (при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.6. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится Оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится Оператор.

6.7. Порядок уничтожения или обезличивания персональных данных (уничтожение или обезличивание части персональных данных, если это допускается материальным носителем), может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

7. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой с использованием средств автоматизации

7.1. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

7.2. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

7.3. Размещение информационной системы, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

7.4. Компьютеры и(или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 4 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, **запрещается.**

7.5. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, **запрещается.**

8. Общие требования по защите персональных данных в

автоматизированных системах

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

8.2. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

б) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

8.3. При обработке персональных данных в информационной системе разработчиками и администратором системы должны обеспечиваться:

а) обучение лиц, использующих средства защиты информации, применяемые в информационной системе, правилам работы с ними;

б) учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

д) описание средств защиты персональных данных.

8.4. Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

9. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации

9.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учету. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

9.2. Учет и выдачу съемных носителей персональных данных по прилагаемой форме осуществляют сотрудники группы АСУ. Работники Института получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета (приложение № 1 к настоящей Инструкции). По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

9.3. Запрещается:

- хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

9.4. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения директора Института.

9.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных.

9.6. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт (приложение № 2 к настоящей Инструкции).

Инструкцию разработал:

Менеджер по персоналу Шек Н.В. - 

Приложение 1

ЖУРНАЛ
учета съемных носителей персональных данных

_____

(наименование учреждения)

№ п/п	Метка съемного Носителя (учетный номер)	Фамилия исполнителя	(Получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Примечание*
1						
2						
3						
4						
5						

Должность и Ф.И.О. ответственного за хранение Подпись

Начат «___» _____20_ г.
Окончен «___» _____20_ г.

На____ листах

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

Приложение 2

Утверждаю

_____

«_____»_____20__ г.

АКТ

уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом _____ от_____
№ _____ в составе:

_____

(должности, ФИО)

провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Пояснения
	2	**3**	**4**

Всего съемных носителей _____

(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены

_____

путем (разрезания, демонтажа и т.п.),

_____

измельчены и сданы для уничтожения предприятию по утилизации вторичного сырья

_____ _____

(наименование предприятия) (Дата)

Председатель комиссии Подпись Дата

Члены комиссии
(ФИО) Подпись Дата