**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**АДМИНИСТРАЦИЯ ТРУБЧЕВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**Р А С П О Р Я Ж Е Н И Е**

от 26.10.2015г. № 817-р

г. Трубчевск

|  |
| --- |
| Об утверждении инструкций в сфере защиты персональных данных в администрации Трубчевского муниципального района |
|  |

  В целях исполнения [Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»](http://itsec2012.ru/federalnyy-zakon-ot-27-iyulya-2006-g-n-152-fz-o-personalnyh-dannyh) и в соответствии с [постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211](http://itsec2012.ru/postanovlenie-ot-21-marta-2012-g-n-211) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»:

1. Утвердить:
   1. Прилагаемую Инструкцию № 1 о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные, в администрации Трубчевского муниципального района.
   2. Прилагаемую Инструкцию № 2 пользователя информационных систем персональных данных (АИС, ИСПДн) при обработке персональных данных (ПДн) администрации Трубчевского муниципального района на объектах вычислительной техники.
   3. Прилагаемую Инструкцию № 3 ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в администрации Трубчевского муниципального района.
   4. Прилагаемую [Инструкцию № 4 по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации](http://itsec2012.ru/instrukciya-po-rezervirovaniyu-i-vosstanovleniyu-rabotosposobnosti-tehnicheskih-sredstv-i-programmnogo-obespecheniya-baz-dannyh-sredstv-zaschity-informacii-i-sredstv-kriptograficheskoy-zaschity-informacii-informacionnoy-sisteme-personalnyh-dannyh) в АИС администрации Трубчевского муниципального района.
   5. Прилагаемую [Инструкцию № 5 по организации парольной защиты](http://itsec2012.ru/instrukciya-po-organizacii-parolnoy-zaschity-v-informacionnyh-sistemah-personalnyh-dannyh) в информационных системах персональных данных администрации Трубчевского муниципального района;
2. [Ответственному за организацию обработки](http://itsec2012.ru/prikaz-o-naznachenii-otvetstvennogo-za-organizaciyu-obrabotki-personalnyh-dannyh) ПДн довести настоящее постановление до сотрудников администрации Трубчевского муниципального района.
3. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации Трубчевского муниципального района Тубол С.Н.

**Глава администрации**

**Трубчевского муниципального района И.И. Обыдённов**

Утверждена

распоряжением администрации

Трубчевского муниципального района

от 26.10.2015г. № 817-р

ИНСТРУКЦИЯ № 1

о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные, в администрации Трубчевского муниципального района

Предмет Инструкции.

Данная Инструкция содержит обязательные для всех отраслевых органов администрации Трубчевского муниципального района (далее – Администрация) требования по обеспечению конфиденциальности документов, содержащих персональные данные.

Определение персональных данных

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, другая информация.

Когда 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);

Необходимость согласия субъекта персональных данных или наличие иного законного основания на их обработку

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.

Порядок ведения перечней персональных данных

В отраслевых органах Администрации формируются и ведутся перечни конфиденциальных данных с указанием регламентирующих документов, мест хранения и ответственных за хранение и обработку данных по прилагаемой форме. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

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

(Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены постановлениями Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и [от 15 сентября 2008 г. № 687](http://clck.yandex.ru/redir/dv/*data=url%3Dhttp%253A%252F%252Fwww.zakonprost.ru%252Fcontent%252Fbase%252F124178%26ts%3D1445273737%26uid%3D4194551921430640175&sign=00cc66dccec1f8bd3a219a6cd64e77a6&keyno=1) «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». 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.

Общие правила хранения и передачи персональных данных

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.

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 отраслевого органа формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «[О персональных данных](http://clck.yandex.ru/redir/dv/*data=url%3Dhttp%253A%252F%252Fwww.zakonprost.ru%252Fzakony%252F152-fz-ot-2006-07-27-o-personalnyh%252F%26ts%3D1445273737%26uid%3D4194551921430640175&sign=cc94c588cb7113c67d5477e113fb1469&keyno=1)», «[О порядке рассмотрения обращений граждан Российской Федерации](http://clck.yandex.ru/redir/dv/*data=url%3Dhttp%253A%252F%252Fwww.zakonprost.ru%252Fzakony%252F59-fz-ot-2006-05-02-o-porjadke%252F%26ts%3D1445273737%26uid%3D4194551921430640175&sign=db51a1b4727f6268521f87cd0177feff&keyno=1)», действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

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.

Ответственность за защиту обрабатываемых персональных данных

Сотрудники отраслевых органов Администрации, сотрудники организаций-Операторов или лица, осуществляющие такую обработку по договору с Оператором, а также иные лица, осуществляющие обработку или хранение конфиденциальных данных в Администрации, 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.

Порядок ознакомления с Инструкцией

Сотрудники отраслевых органов Администрации и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией.

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

Условия хранения персональных данных

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.

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.

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.

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.

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.

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).

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).

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

Правила доступа, хранения и пересылки персональных данных

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

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

Размещение информационных систем, 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.

Компьютеры и(или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

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

Общие требования по защите персональных данных в автоматизированных системах

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

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.

При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

а) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, 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 системы защиты персональных данных).

специфические требования по защите персональных данных в отдельных автоматизированных системах

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

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

Организация учета носителей персональных данных

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.

Учет и выдачу съемных носителей персональных данных по прилагаемой форме осуществляют сотрудники отраслевого органа Администрации, на которых возложены функции хранения носителей персональных данных. Сотрудники Администрации получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

Правила использования съемных носителей персональных данных

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.

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 руководителя отраслевого органа Администрации.

Порядок действий при утрате или уничтожении съемных носителей персональных данных

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

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 по прилагаемой форме.

[Пример формы учета персональных данных](http://clck.yandex.ru/redir/dv/*data=url%3Dhttp%253A%252F%252Fwww.zakonprost.ru%252Fcontent%252Fbase%252Fpart%252F644085%26ts%3D1445273737%26uid%3D4194551921430640175&sign=303bd1ea53aa91d7e3b494bf4e28be0e&keyno=1)

ПЕРЕЧЕНЬ   
персональных данных, обрабатываемых в отраслевых органах   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
наименование учреждения

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
наименование отраслевого органа

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| N п/п | Наименование (вид, типовая форма) документов с персональными данными | Регламентирующие документы (Наименование, дата, номер) | Наименование информационной системы/ без использования средств автоматизации | Отдел | Место хранения (комната) | ФИО ответственных за обработку и хранение |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Должность и ФИО начальника отраслевого органа |  | Подпись |
|  |  |  |
| Должность и ФИО ответственного за защиту персональных данных |  | Подпись |

[Пример формы журнала учета съемных носителей](http://clck.yandex.ru/redir/dv/*data=url%3Dhttp%253A%252F%252Fwww.zakonprost.ru%252Fcontent%252Fbase%252Fpart%252F644086%26ts%3D1445273737%26uid%3D4194551921430640175&sign=ac4509c48f03d713f42a468618538e93&keyno=1)

ЖУРНАЛ   
учета съемных носителей персональных данных   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
наименование отраслевого органа

Начат "\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 200\_ г.

Окончен "\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 200\_ г.

На \_\_\_\_\_\_листах

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Должность и ФИО ответственного за хранение |  | Подпись |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| N п/п | Метка съемного носителя (учетный номер) | Фамилия исполнителя | (Получил, вернул, передал) | Дата записи информации | Подпись исполнителя | Примечание <\*> |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |

<\*> Причина и основание окончания использования (N и дата отправки адресату или распоряжения о передаче, N и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

[Пример акта](http://clck.yandex.ru/redir/dv/*data=url%3Dhttp%253A%252F%252Fwww.zakonprost.ru%252Fcontent%252Fbase%252Fpart%252F644089%26ts%3D1445273737%26uid%3D4194551921430640175&sign=a0add965404fedd47d2e9f4c3dbca597&keyno=1)

|  |  |  |
| --- | --- | --- |
| "УТВЕРЖДАЮ" | | |
|  |  |  |
| "\_\_" \_\_\_\_\_\_\_\_\_\_ 200 г. | | |

АКТ   
уничтожения съемных носителей персональных данных

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Комиссия, наделенная полномочиями распоряжение (приказом) | |  | | от |  |
| N | в составе: |  |  |  |  |
|  |  |  |  |  |  |
| (должности, ФИО) | | | | | |
| провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению: | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| N 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 |
|  |  |  |

С инструкцией ознакомлен (ы):

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

Утверждена

распоряжением администрации

Трубчевского муниципального района

от 26.10.2015г. № 817-р

ИНСТРУКЦИЯ № 2

пользователя информационных систем персональных данных (АИС, ИСПДн) при обработке персональных данных (ПДн) администрации Трубчевского муниципального района на объектах вычислительной техники

1.Общие положения

1.1.Данная Инструкция определяет основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) администрации Трубчевского муниципального района (далее – Администрация).

1.2.Пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ.

1.3.Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации).

2.Основные обязанности пользователя:

2.1.Выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции.

2.2.При работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами.

2.3.Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке.

2.4.После окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ПЭВМ.

2.5.Оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальника обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ.

2.6.Не допускать "загрязнение" ПЭВМ посторонними программными средствами.

2.7.Знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий.

2.8.Знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий.

2.9.Помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе.

2.10.Знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов.

2.11.При применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

3.Требования к антивирусной безопасности

3.1.При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

3.2.В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

​ - приостановить работу;

​ - немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;

​ - оценить необходимость дальнейшего использования файлов, зараженных вирусом;

​ - провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

4.Пользователю запрещается:

4.1.Записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;

4.2.Удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

4.3.Самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;

4.4.Самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

4.5.Осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;

4.6.Сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

4.7.Отключать (блокировать) средства защиты информации;

4.8.Производить какие-либо изменения в подключении и размещении технических средств;

4.9.Производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.

4.10.Оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

5.Права пользователя ПЭВМ:

5.1.Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.

5.2.Обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

6.Пользователи ПЭВМ несут ответственность за:

6.1.Надлежащее выполнение требований настоящей Инструкции;

6.2.Соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;

6.3.Сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;

6.4.Сохранность персональных данных.

6.5. Согласно статье 90 Трудового кодекса Российской Федерации «Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника»: лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации и (или) совершенные лицом с использованием своего служебного положения подпадает под действие статьи 137 Уголовного кодекса Российской Федерации «Нарушение неприкосновенности частной жизни».

Отказ в предоставлении гражданину информации. Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан подпадает под действие статьи 140.

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации подпадает под действие статьи 272 Уголовного кодекса Российской Федерации «Неправомерный доступ к компьютерной информации».

Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

С инструкцией ознакомлен (ы):

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

Утверждена

распоряжением администрации

Трубчевского муниципального района

от 26.10.2015г. № 817-р

ИНСТРУКЦИЯ № 3

ответственного за обеспечение безопасности персональных данных

в информационных системах персональных данных

в администрации Трубчевского муниципального района

I. Общие положения

1. Настоящая Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в администрации Трубчевского муниципального района (далее – Администрация) разработана на основе Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных».

2. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных в Администрации в своей деятельности руководствуется Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», другими законодательными и нормативными правовыми актами по вопросам обработки и защиты персональных данных.

II. Обязанности ответственного за обеспечение безопасности персональных данных

в информационных системах персональных данных в Администрации

3. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных:

- составляет и поддерживает в актуальном состоянии перечень должностных лиц, доступ которых к персональным данным необходим для выполнения ими своих служебных обязанностей;

- поддерживает необходимый уровень защищенности персональных данных при их обработке в информационных системах персональных данных, функционирующих в Администрации;

- участвует в определении полномочий пользователей информационных систем персональных данных, функционирующих в Администрации (оформлении разрешительной системы доступа);

- осуществляет учет документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения;

- блокирует доступ к персональным данным при обнаружении нарушения порядка их обработки;

- информирует администратора безопасности в информационных системах персональных данных Администрации о фактах несанкционированного доступа к персональным данным;

- осуществляет контроль мероприятий по установке и настройке средств защиты информации;

- поддерживает в актуальном состоянии правовые акты Администрации в области защиты персональных данных;

- осуществляет подготовку отчетов о состоянии работ по обеспечению защиты персональных данных в Администрации.

III. Права ответственного за обеспечение безопасности персональных данных

в информационных системах персональных данных

в Администрации

4.Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных имеет право:

- требовать от сотрудников Администрации соблюдения действующего законодательства в области защиты персональных данных;

- контролировать в Администрации осуществление мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006г №152-ФЗ «О персональных данных».

IV. Ответственность лица, назначенного ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных

5. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность за невыполнение или халатное выполнение обязанностей по организации, контролю и обеспечению выполнения требований законодательства Российской Федерации в области обработки и защиты персональных данных.

С инструкцией ознакомлен (ы):

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

Утверждена

распоряжением администрации

Трубчевского муниципального района

от 26.10.2015г. № 817-р

**ИНСТРУКЦИЯ № 4**

по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации в АИС администрации Трубчевского муниципального района

1. **Общие положения**

1.1.         Настоящая инструкция (далее – Инструкция) по резервирования и восстановления работоспособности технических средств (далее – ТС), программного обеспечения (далее – ПО), баз данных (далее – БД), средств защиты информации (далее – СЗИ)и средств криптографической защиты информации (далее – СКЗИ) информационных систем персональных данных (далее – АИС) в администрации Трубчевского муниципального района (далее – Администрация) определяет действия, связанные с функционированием технических и программных средств АИС  и системы защиты персональных данных (далее – СЗПДн).

1.2.         Инструкция разработана в соответствии с [руководящими и нормативными документами регуляторов Российской Федерации](http://itsec2012.ru/normativno-pravovye-akty-po-informacionnoy-bezopasnosti) в области защиты персональных данных.

1.3.         Целью данной Инструкции является превентивная защита элементов АИС  и СЗПДн от предотвращения потери защищаемой информации.

1.4.         Задачами данной Инструкции являются:

- определение мер защиты от потери информации;

- определение действий восстановления технических и программных средств АИС  и СЗПДн в случае потери информации.

1.5.         Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам АИС, в том числе на ответственного за обеспечение безопасности персональных данных информационных систем персональных данных Администрации и администратора АИС  (далее – администратор системы), имеющих доступ к техническим и программным средствам СЗПДн в рамках своих полномочий, при возникновении аварийных ситуаций, в том числе:

- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных;

- системы контроля физического доступа.

1.6.         Пользователем АИС  (далее – Пользователь) является сотрудник Администрации, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных (далее – ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению, данным и СЗИ АИС.

1.7.         Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов АИС  или СЗПДн, предоставляемых пользователям, а также потерей защищаемой информации.

1. **Порядок реагирования на инцидент**

2.1.         Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;

- в результате преднамеренных действий пользователей и третьих лиц;

- в результате нарушения правил эксплуатации технических средств АИС  и СЗПДн;

- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.2.         Все действия в процессе реагирования на Инцидент должны документироваться ответственным за обеспечение безопасности персональных данных информационных систем персональных данных Администрации и администратором системы в «[Журнал учета событий информационной безопасности](http://itsec2012.ru/zhurnal-ucheta-sobytiy-informacionnoy-bezopasnosti-1)».

2.3.        В кратчайшие сроки, не превышающие одного рабочего дня, ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Администрации  и администратор системы предпринимают меры по восстановлению работоспособности.

2.4.         Предпринимаемые меры, по возможности, согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.

1. **Технические меры**

3.1.         К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения АИС;

- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных;

- системы контроля физического доступа.

3.2.         Системы жизнеобеспечения АИС  включают:

-  пожарные сигнализации и системы пожаротушения;

- системы вентиляции и кондиционирования;

- системы резервного питания.

3.3.         Все [критичные помещения](http://itsec2012.ru/ob-opredelenii-granic-kontroliruemoy-zony-i-trebovaniy-k-ee-bezopasnosti) Администрации (помещения, в которых размещаются элементы АИС  и СЗПДн) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.4.         Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств АИС  в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.5.         Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы АИС  и СЗПДн, сетевое и коммуникационное оборудование, а также наиболее критичные АРМ должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

- дублированные системы электропитания в устройствах (серверы, активное сетевое оборудование и т. д.);

- резервные линии электропитания в пределах комплекса зданий;

- аварийные электрогенераторы.

3.6.         Системы обеспечения отказоустойчивости:

- кластеризация;

- технология RAID.

3.7.         Для обеспечения отказоустойчивости критичных компонентов АИС  при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации.

3.8.         Для наиболее критичных компонентов АИС  должны использоваться территориально удаленные системы кластеров.

3.9.         Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.10.    Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

1. **Организационные меры**

4.1.         Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых ПДн – согласно инструкции по обеспечению безопасности ПДн;

- для технологической информации – не реже раза в месяц;

- эталонные копии программного обеспечения (ОС, штатное и специальное ПО, программные СЗИ), с которых осуществляется их установка на элементы АИС  – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

4.2.         Данные о проведении процедуры резервного копирования должны отражаться в специально созданном журнале учета.

4.3.         Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

4.4.         Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

4.5.         Носители должны храниться не менее года для возможности восстановления данных.

С инструкцией ознакомлен (ы):

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

Утверждена

распоряжением администрации

Трубчевского муниципального района

от 26.10.2015г. № 817-р

**ИНСТРУКЦИЯ № 5**

по организации парольной защиты в информационных системах

персональных данных администрации Трубчевского муниципального района

1. **Общие положения**

1.1.        Настоящая инструкция (далее – Инструкция) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаление учетных записей пользователей) в информационной системе персональных (далее – ИСПДн) в администрации Трубчевского муниципального района (далее – Администрация).

1.2.         Настоящая Инструкция разработана в соответствии с [руководящими и нормативными документами регуляторов Российской Федерации](http://itsec2012.ru/normativno-pravovye-akty-po-informacionnoy-bezopasnosti) в области защиты персональных данных.

1.3.         Пользователем ИСПДн (далее – Пользователь) является сотрудник Администрации, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных (далее – ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации ИСПДн (далее – СЗИ).

1.4.        Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн и контроль над действиями Пользователей в ИСПДн осуществляет [ответственный за обеспечение безопасности персональных данных](http://itsec2012.ru/o-naznachenii-otvetstvennogo-za-obespechenie-bezopasnosti-personalnyh-dannyh-informacionnyh-sistem-personalnyh-dannyh-1) в Администрации (далее – Ответственный).

1.5.         Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на автоматизированных рабочих местах (далее – АРМ) Пользователей осуществляет администратор ИСПДн в Администрации (далее –Администратор).

1. **Организация парольной защиты**

2.1.         Личные пароли должны создаваться Пользователями самостоятельно.

2.2.         В случае формирования личных паролей Пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного и Администратора в ИСПДн и на АРМ Пользователей соответственно.

2.3.         Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

2.4.         Внеплановая смена личного пароля Пользователя или удаление учетной записи в случае прекращения его полномочий (увольнение, переход на другую должность в ИСПДн и т.п.) должна производиться Администратором и Ответственным немедленно после окончания последнего сеанса работы Пользователя в АРМ и в ИСПДн соответственно.

2.5.         В ИСПДн устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) Пользователя, равное 7, после чего учетная запись блокируется.

2.6.         Разблокирование учетной записи осуществляется Администратором и Ответственный для учетных записей Пользователя для АРМ и для ИСПДн соответственно.

2.7.         После 15 минут бездействия (неактивности) Пользователя в АРМ или ИСПДн происходит автоматическое блокирование сеанса доступа в АРМ и ИСПДн соответственно.

1. **Требования к формированию паролей**

Пользователи при формировании паролей должны руководствоваться следующими требованиями:

3.1.         Длина пароля должна быть не менее 8 символов.

3.2.         В пароле должны обязательно присутствовать символы не менее 3-х категорий из следующих:

* буквы в верхнем регистре;
* буквы в и нижнем регистре;
* цифры;
* специальные символы, не принадлежащие алфавитно-цифровому набору (например, !, @, #, $, &, \*, % и т.п.).

3.3.         Пароль не должен включать в себя легко вычисляемые сочетания символов (например, «112», «911» и т.п.), а также общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.).

3.4.         Пароль не должен содержать имя учетной записи Пользователя или наименование его АРМ, а также какую-либо его часть.

3.5.         Пароль не должен основываться на именах и датах рождения Пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о Пользователе.

3.6.         Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «1111111», «wwwww» и т.п.).

3.7.         Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567», «qwerty» и т.п.).

3.8.         При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

1. **Правила ввода паролей**

Пользователи во время процедуры аутентификации (ввода логина и пароля) на АРМ и в ИСПДн должны руководствоваться следующими правилами:

4.1.         Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

4.2.         Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и пр.).

4.3.         В случае блокировки учетной записи Пользователя после превышения попыток ввода данных аутентификации (логина и пароля) в АРМ или ИСПДн, Пользователю необходимо уведомить Администратора или Ответственный соответственно для проведения процедуры генерации нового пароля.

1. **Обязанности**

Пользователи ИСПДн обязаны:

5.1.         Четко знать и строго выполнять требования настоящей инструкции и других руководящих документов Администрации по парольной защите.

5.2.         Своевременно сообщать Ответственному и Администратору об утере, компрометации и несанкционированном изменении сроков действия паролей в АРМ и ИСПДн соответственно.

5.3.         Ознакомиться под роспись с перечисленными в настоящей инструкции требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

1. **Ответственность**

6.1.         Пользователь несет персональную ответственность за сохранность данных аутентификации (персонального логина и пароля) к АРМ и к ИСПДн.

С инструкцией ознакомлен (ы):

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)