ПОСТАНОВЛЕНИЕ

АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО ГОРОДСКОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ

24 апреля 2018 г. **г. Изобильный** № 532

Об утверждении внутренних нормативно-правовых актов по защите персональных данных в администрации Изобильненского городского округа Ставропольского края

Для обеспечения безопасности персональных данных при их обработке в администрации Изобильненского городского округа Ставропольского края, во исполнение требований Федерального закона от 27 июля 2006 года № 152 «О персональных данных», постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 г. № 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», администрация Изобильненского городского округа Ставропольского края

ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые:

1.1. Инструкцию системного администратора информационных систем персональных данных по обеспечению безопасности персональных данных в администрации Изобильненского городского округа Ставропольского края;

1.2. Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в администрации Изобильненского городского округа Ставропольского края;

1.3. Инструкцию по организации антивирусной защиты в администрации Изобильненского городского округа Ставропольского края;

1.4. Инструкцию по порядку учета и хранению документов, содержащих персональные данные, в администрации Изобильненского городского округа Ставропольского края;

1.5. Инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в администрации Изобильненского городского округа Ставропольского края;

1.6. Инструкцию по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в администрации Изобильненского городского округа Ставропольского края;

1.7. Инструкцию пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в администрации Изобильненского городского округа Ставропольского края;

1.8. Регламент порядка действий сотрудников администрации Изобильненского городского округа Ставропольского края, при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

2. Ответственному за организацию обработки персональных данных довести до сведения всех сотрудников, обрабатывающих персональные данные, положения утверждаемых нормативных правовых актов.

3. Контроль за выполнением настоящего постановления оставляю за собой.

4. Настоящее постановление вступает в силу со дня подписания и распространяется на правоотношения возникшие с 01 января 2018 года.

Глава Изобильненского городского
округа Ставропольского края В.И.Козлов

УТВЕРЖДЕНА

постановлением администрации
Изобильненского городского
округа Ставропольского края
от 24 апреля 2018 г. № 532

ИНСТРУКЦИЯ
системного администратора информационных систем персональных данных по обеспечению безопасности персональных данных в администрации Изобильненского городского округа Ставропольского края

1. Общие положения

1.1. Настоящая Инструкция определяет обязанности, полномочия и ответственность системного администратора информационных систем персональных данных (далее ИСПДн) по обеспечению безопасности персональных данных в администрации Изобильненского городского округа Ставропольского края (далее – администрация).

1.2. Администратор ИСПДн (далее – администратор) назначается постановлением администрации.

1.3. Администратор ИСПДн подчиняется руководителю администрации.

1.4. Администратор ИСПДн в своей работе руководствуется настоящей Инструкцией и Положением о защите персональных данных, руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России и внутренними регламентирующими документами по защите информации в администрации.

1.5. Администратор ИСПДн отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

2. Обязанности по обеспечению безопасности информации

Администратор ИСПДн обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Ознакомить всех пользователей ИСПДн с внутренними нормативно-правовыми актами по обеспечению безопасности персональных данных (под роспись).

2.3. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

программного обеспечения автоматизированных рабочих мест (далее – АРМ) и серверов (операционные системы, прикладное и специальное ПО);

аппаратных средств;

аппаратных и программных средств защиты.

2.4. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.5. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов (если не назначен другой ответственный).

2.6. Обеспечивать функционирование и поддерживать работоспособность средств защиты.

2.7. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.8. Осуществлять регистрацию пользователей, выдачу временных паролей пользователей, осуществлять контроль за правильностью использования пароля пользователем ИСПДн.

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.11. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт.

2.12. Присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними физическими лицами и Компаниями.

2.13. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Ответственность

В случае нарушения положений настоящей Инструкции администратор несёт ответственность в соответствии с действующим законодательством.

УТВЕРЖДЕНА

постановлением администрации
Изобильненского городского
округа Ставропольского края
от 24 апреля 2018 г. № 532

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в администрации Изобильненского городского округа Ставропольского края

1. Назначение и область действия

Данная Инструкция определяет действия, связанные с мерами и средствами поддержания непрерывной работы и восстановления работоспособности информационных систем в администрации Изобильненского городского округа Ставропольского края (далее – администрация).

Настоящая Инструкция регламентирует:

меры защиты от потери информации;

действия по восстановлению в случае потери информации.

Действие настоящей Инструкции распространяется на администраторов информационных систем, ответственных за резервное копирование информации.

Меры обеспечения надежной работы и восстановления ресурсов при возникновении инцидентов.

1.1. Технические меры.

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

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

пожарные сигнализации и системы пожаротушения;

системы вентиляции и кондиционирования;

системы резервного питания.

Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, 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;

резервные линии электропитания в пределах комплекса зданий;

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

1.2. Организационные меры.

Резервное копирование и хранение данных должно осуществлять на периодической основе:

для обрабатываемых персональных данных – не реже раза в неделю или по требованию пользователя ИСПДн;

для системной информации – не реже раза в месяц;

эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования должны отражаться в специально созданном Журнале учета согласно приложению к инструкции.

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

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

Носители и резервные копии данных должны храниться не менее года для возможности восстановления данных.

Порядок проведения резервирования информации

Перед проведением процедуры резервного копирования необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

Резервирование информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия

таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

Все файлы, входящие в состав резервной копии, должны архивироваться в один архив с присвоением имени архива в формате время_дата (например, 18.00_21.11.2011).

Архивация может производиться как штатными средствами, поставляемыми в составе специализированного программного обеспечения для построения информационной системы, так и сторонним программным обеспечением (например, 7zip, WinRar).

Резервные копии должны сохраняться на носители, не входящие в состав технических средств информационной системы персональных данных (внешние жесткие диски, CD/DVD диски, flash диски).

После завершения процедуры резервного копирования информации и записи резервной копии на носитель, необходимо поместить носитель с резервной копией в специально отведённое для хранения место и проставить соответствующую отметку в Журнале.

1.3. Порядок проведения восстановления информации

Перед проведением процедуры восстановления информации необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

Восстановление информации следует проводить из наиболее актуальной резервной копии.

В случае, если специализированное программное обеспечение для построения информационной системы не позволяет работать с заархивированными резервными копиями, то перед восстановлением информации необходимо разархивировать файлы резервной копии при помощи стороннего программного обеспечения (например 7zip, WinRar).

Восстановление информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

После завершения процедуры восстановления необходимо убедиться в работоспособности информационной системы персональных данных.

В случае успешного восстановления оповестить пользователей информационной системы о возможности продолжения работы. В противном случае необходимо изучить документацию, прилагаемую к программному обеспечению либо обратиться в службу технической поддержки.

1.4. Ответственность

Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение

к инструкции о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в администрации Изобильненского городского округа Ставропольского края, утвержденной постановлением администрации Изобильненского городского округа Ставропольского края
от 24 апреля 2018 г. № 532

Журнал
учета резервного копирования и восстановления данных в администрации Изобильненского городского округа Ставропольского края

Дата проведения резервного копирования/восстановления	Наименование резервной копии	Наименование информационной системы/базы данных	Ф.И.О., подпись ответственного

УТВЕРЖДЕНА

постановлением администрации
Изобильненского городского
округа Ставропольского края
от 24 апреля 2018 г. № 532

ИНСТРУКЦИЯ
по организации антивирусной защиты в администрации Изобильненского городского округа Ставропольского края

1. Общие положения

1.1. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в администрации Изобильненского городского округа Ставропольского края (далее - Администрация) и предотвращения возникновения фактов заражения вредоносным программным обеспечением.

1.2. Данная Инструкция распространяется на всех пользователей и администраторов информационных систем персональных данных (далее – ИСПДн) в Администрации.

2. Установка и обновление антивирусных средств

2.1. Установка и настройка антивирусных средств осуществляется только Администратором информационной системы персональных данных.

2.2. Обновление антивирусных баз осуществляется по расписанию в автоматическом режиме, либо вручную при необходимости.

3. Требования к проведению мероприятий по антивирусной защите

3.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, flash дисках, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

3.2. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие заражения вредоносным программным обеспечением.

3.3. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

3.4. Особое внимание следует обратить на недопустимость использования съёмных носителей, принадлежащих лицам, временно допущенным к работе на ЭВМ. Работа этих лиц должна проводиться под непосредственным контролем сотрудника или ответственного за информационную безопасность.

3.5. Ежедневно, в начале работы, должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех загружаемых в память файлов персонального компьютера.

3.6. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

3.7. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

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.).

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора информационной системы персональных данных;

провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса пользователь или Администратор информационной системы персональных данных должны провести внеочередной антивирусный контроль.

5. Ответственность при организации антивирусной защиты

5.1. Ответственность за организацию антивирусной защиты возлагается на Администратора информационной системы персональных данных.

5.2. Ответственность за выполнение требований данной Инструкции возлагается на пользователей и Администратора информационной системы персональных данных.

5.3. Периодический контроль за соблюдением положений данной Инструкции возлагается на Администратора информационной системы персональных данных.

УТВЕРЖДЕНА

постановлением администрации
Изобильненского городского
округа Ставропольского края
от 24 апреля 2018 г. № 532

ИНСТРУКЦИЯ
по порядку учета и хранению документов, содержащих персональные данные, в администрации Изобильненского городского округа Ставропольского края

1. Общие положения

1.1. Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при работе с документами, содержащими персональные данные.

1.2. Действие настоящей Инструкции распространяется на сотрудников администрации Изобильненского городского округа Ставропольского края (далее – Администрация), допущенных к обработке персональных данных.

2. Порядок учета, хранения и обращения с документами, которые содержат персональные данные

2.1. Все находящиеся на хранении и в обращении документы с персональными данными в Администрации подлежат учёту.

2.2. Каждый документ, личное дело или журнал должны иметь уникальный учетный номер.

2.3. Учет и выдачу документов с персональными данными осуществляют сотрудники структурных подразделений, на которых возложены функции хранения документов, содержащих персональные данные. Факт выдачи документов фиксируется в журнале учета согласно приложению.

2.4. При работе с документами, которые содержат персональные данные необходимо:

2.4.1. Соблюдать требования настоящей Инструкции.

2.4.2. Использовать полученные документы исключительно для выполнения своих служебных обязанностей.

2.4.3. Ставить в известность ответственного за обработку персональных данных о любых фактах нарушения требований настоящей Инструкции.

2.4.4. Бережно относиться к документам, содержащим персональные данные.

2.4.5. Обеспечивать физическую безопасность документов всеми разумными способами.

2.4.6. Обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях

2.4.7. Извещать ответственного за организацию обработки персональных данных о фактах утраты (кражи) документов, содержащих персональные данные.

2.4.8. Осуществлять вынос документов с персональными данными для непосредственной передачи адресату только с письменного разрешения руководителя.

2.4.9. При передаче персональных данных передаётся минимальный объем данных, который необходим для выполнения служебных обязанностей адресата.

2.4.10. В случае утраты или уничтожения документов, которые содержат персональные данные либо разглашении содержащихся в них сведений, немедленно ставится в известность руководитель Администрации. Отметки об утрате вносятся в журнал учета документов с персональными данными.

2.4.11. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные документы с персональными данными информации изымаются.

3. Работа с журналом регистрации посетителей

3.1. Журнал регистрации посетителей необходим исключительно в целях контроля посещаемости.

3.2. В Журнале учёта посещаемости разрешается фиксация следующих персональных данных:

фамилия, имя, отчество;

наименование и номер документа, удостоверяющего личность (паспорт, водительское удостоверение, удостоверение личности и т.д.);

3.3. Порядок учёта, хранения и обращения с журналом регистрации посетителей осуществляется в соответствии с п. 2 настоящей инструкции.

3.4. В случае окончания журнала, его необходимо сдать в архив или уничтожить.

4. Запрещается

4.1. Использовать документы с персональными данными в личных целях.

4.2. Передавать документы с персональными данными третьим лицам без соответствующего разрешения руководителя Администрации.

4.3. Хранить документы с персональными данными вместе с документами с открытой информацией на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

4.4. Выносить документы с персональными данными из служебных помещений для работы с ними на дому и т. д.

4.5. Оставлять документы с персональными данными без присмотра.

4.6. Изготавливать и хранить копии паспортов или иных документов, удостоверяющих личность, за исключением случаев, предусмотренных законодательством.

5. Ответственность

Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение

к инструкции по порядку учета и хранению документов, содержащих персональные данные, в администрации Изобильненского городского округа Ставропольского края, утвержденной постановлением администрации Изобильненского городского округа Ставропольского края от 24 апреля 2018 г. № 532

Администрация Изобильненского городского округа Ставропольского края
Журнал учета и выдачи документов с персональными данными

ФИО и должность лица или наименование органа, запрашивающего личные данные	Цель выдачи документа	Перечень наименований запрашиваемых документов	Дата выдачи документа, подпись лица, получившего документ	Дата возврата документа, подпись лица, получившего документ

Приложение

к инструкции по порядку учета и хранению документов, содержащих персональные данные, в администрации Изобильненского городского округа Ставропольского края, утвержденной постановлением администрации Изобильненского городского округа Ставропольского края от 24 апреля 2018 г. № 532

Администрация Изобильненского городского округа Ставропольского края
Журнал регистрации посетителей

ФИО посетителя	Наименование и номер документа, удостоверяющего личность

УТВЕРЖДЕНА

постановлением администрации
Изобильненского городского
округа Ставропольского края
от 24 апреля 2018 г. № 532

ИНСТРУКЦИЯ
по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в администрации Изобильненского городского округа Ставропольского края

1. Общие положения

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования средств криптографической защиты информации (далее-СКЗИ) и криптографических ключей, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации в администрации Изобильненского городского округа Ставропольского края (далее – администрация).

1.2. Пользователь должен выполнять все требования настоящей Инструкции, правила, изложенные в эксплуатационной документации на СКЗИ, а также другие документы, регламентирующие порядок работы с СКЗИ.

Обязанности Пользователя :

1.3. Пользователь обязан соблюдать требования по обеспечению безопасности функционирования СКЗИ.

1.4. Пользователь обязан обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей.

1.5. Пользователь обязан сдать носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, ответственному за обработку персональных данных.

1.6. Пользователь обязан сдать носители ключевой информации (далее – НКИ) по окончании срока действия сертификата ключа, а также в случае компрометации ключа.

1.7. Пользователь обязан немедленно уведомлять ответственного за обработку персональных данных о компрометации криптографических ключей.

1.8. Пользователь обязан немедленно уведомлять ответственного за обработку персональных данных о фактах утраты или недостачи СКЗИ, НКИ.

Порядок обращения со средствами криптографической защиты информации:

1.9. Монтаж и установка СКЗИ осуществляются только уполномоченным лицом, либо организацией, имеющей необходимые лицензии.

1.10. Все СКЗИ и НКИ должны учитываться в журнале согласно приложению.

1.11. Служебные помещения, в которых размещаются СКЗИ, должны оборудоваться охранной сигнализацией, по убытии сотрудников закрываться и сдаваться под охрану.

1.12. Для хранения носителей ключевой информации помещения обеспечиваются сейфами (металлическими шкафами).

1.13. Несанкционированное изготовление дубликатов ключей запрещено. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

1.14. К эксплуатации СКЗИ допускаются лица, изучившие правила пользования данным СКЗИ.

1.15. Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

2. Порядок обращения с ключами ЭЦП

2.1. Криптографический ключ применяется для подписания (проверки электронной цифровой подписи) электронных документов до окончания срока его действия или наступления события, трактуемого как компрометация криптографических ключей.

2.2. Изготовление и выдача ключей ЭЦП осуществляется только Удостоверяющим центром.

2.3. Выработанные закрытые (конфиденциальные) криптографические ключи хранятся исключительно в электронном виде на цифровых носителях информации, которые получают статус НКИ.

2.4. НКИ являются объектами особой важности, т.к. они содержат информацию, предназначенную для гарантированной идентификации владельца ключа, защиты электронного документа от подделки и обеспечения конфиденциальности документа.

2.5. Владельцы ключей несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.

2.6. Для хранения носителей ключевой информации Пользователь должен быть обеспечен личным сейфом.

3. Запрещается

3.1. Осуществлять несанкционированное и без учётное копирование ключевых данных.

3.2. Хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность.

3.3. Передавать НКИ третьим лицам.

3.4. Во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ).

3.5. Хранить на НКИ какую-либо информацию, кроме ключевой.

3.6. Использование выведенных из действия криптографических ключей.

4. Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

4.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

утрата (хищение) НКИ, в том числе – с последующим их обнаружением;

увольнение (переназначение) сотрудников, имевших доступ к ключевой информации;

передача закрытых (конфиденциальных) ключей по линии связи в открытом виде;

нарушение правил хранения криптографических ключей;

вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

отрицательный результат при проверке наложенной ЭЦП;

несанкционированное или без учётное копирование ключевой информации;

все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

4.2. При наступлении любого из перечисленных выше событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) в Удостоверяющий центр, производивший генерацию ключей ЭЦП.

4.3. При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.

4.4. Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь получает в Удостоверяющем центре новые ключи ЭЦП.

5. Ответственность Пользователя

5.1. Владелец ключа несет персональную ответственность за конфиденциальность личных ключевых носителей.

5.2. В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь несёт ответственность в соответствии с действующим Законодательством Российской Федерации.

УТВЕРЖДЕНА

постановлением администрации
Изобильненского городского
округа Ставропольского края
от 24 апреля 2018 г. № 532

ИНСТРУКЦИЯ
по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в администрации Изобильненского городского округа Ставропольского края

1. Общие положения

1.1. Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при их хранении на съемных носителях.

1.2. Действие настоящей Инструкции распространяется на сотрудников администрации Изобильненского городского округа Ставропольского края (далее - Администрация), допущенных к обработке персональных данных.

2. Основные термины, сокращения и определения

2.1. Администратор информационной системы персональных данных – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.

2.2. АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

2.3. ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

2.4. ИС – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

2.5. Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации.

2.6. ПК – персональный компьютер.

2.7. ПО – программное обеспечение вычислительной техники.

2.8. ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.9. Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИС понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью Администрации и подвергаются регулярной ревизии и контролю.

3.3. Носители конфиденциальной информации предоставляются сотрудникам Администрации на основании письменного разрешения руководителя Администрации при:

необходимости выполнения вновь принятым работником своих должностных обязанностей;

возникновения у сотрудника Администрации производственной необходимости.

4. Порядок учета, хранения и обращения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации

4.1. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в Администрации подлежат учёту.

4.2. Каждый съемный носитель с записанными на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляет ответственный за организацию обра-

ботки персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации согласно приложению.

5. При использовании сотрудниками носителей конфиденциальной информации необходимо

5.1. Соблюдать требования настоящей Инструкции.

5.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.

5.3. Ставить в известность ответственного за обработку персональных данных о любых фактах нарушения требований настоящей Инструкции.

5.4. Бережно относиться к носителям конфиденциальной информации (персональных данных).

5.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами.

5.6. Извещать ответственного за обработку персональных данных о фактах утраты (кражи) носителей конфиденциальной информации.

5.7. Перед работой проверять носители конфиденциальной информации на наличие вредоносного ПО.

5.8. Осуществлять вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату только с письменного разрешения руководителя.

5.9. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных носителях осуществляется в порядке, установленном для документов данного типа.

5.10. В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность руководитель Администрации. На утраченные носители составляется акт. Соответствующие

отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

5.11. Съемные носители конфиденциальной информации (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.

5.12. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются.

6. Запрещается

6.1. Использовать носители конфиденциальной информации в личных целях.

6.2. Передавать носители конфиденциальной информации другим лицам (за исключением администраторов ИС).

6.3. Хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

6.4. Выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

7. Ответственность

Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Журнал выдачи носителей конфиденциальной информации (каждая последующая страница Журнала)

Инвентарный номер носителя	Сотрудник, выдавший носитель (Ф.И.О., подпись, дата)	Сотрудник, получивший носитель (Ф.И.О., подпись, дата)	Возврат носителя. Сотрудник, получивший носитель (Ф.И.О., подпись, дата)

Приложение

к инструкции по порядку учета и хранению съёмных носителей конфиденциальной информации (персональных данных) в администрации Изобильненского городского округа Ставропольского края, утвержденной постановлением администрации Изобильненского городского округа Ставропольского края от 24 апреля 2018 г. № 532

Администрация Изобильненского городского округа Ставропольского края
Журнал учёта носителей конфиденциальной информации
(1-ая страница Журнала)

Инвентарный номер носителя	Поставлен на учёт (Дата постановки, Ф.И.О., подпись ответственного)	Снят с учёта (Дата снятия, причина снятия, Ф.И.О., подпись ответственного)

УТВЕРЖДЕНА

постановлением администрации
Изобильненского городского
округа Ставропольского края
от 24 апреля 2018 г. № 532

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в администрации Изобильненского городского округа Ставропольского края

1. Общие положения

1.1. Пользователь информационной системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных в информационных системах персональных данных в администрации Изобильненского городского округа Ставропольского края (далее – администрация).

1.2. Пользователем является каждый работник администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России и другими внутренними нормативно - правовыми документами администрации по защите информации.

2. Обязанности пользователя

2.1. Пользователь обязан:

знать и выполнять требования настоящей Инструкции и других внутренних нормативно – правовых документов, по защите персональных данных;

выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией;

знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации,

обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов;

соблюдать требования парольной политики;

соблюдать правила при работе в сетях общего доступа и международного обмена – Интернет;

экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нём информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.2. Обо всех выявленных нарушениях, связанных с информационной безопасностью в администрации, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к администратору информационной системы персональных данных или ответственном за обработку персональных данных.

2.3. Для получения консультаций по вопросам работы и настройке элементов информационной системы персональных данных необходимо обращаться к администратору информационной системы персональных данных.

3. Пользователям запрещается:

разглашать защищаемую информацию третьим лицам;

копировать защищаемую информацию на внешние носители без письменного разрешения руководителя структурного подразделения или администрации;

самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

несанкцинонированно открывать общий доступ к ресурсам;

запрещено подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;

отключать (блокировать) средства защиты информации;

обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационной системе персональных данных;

сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системе персональных данных;

привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с Администратором информационной системы персональных данных.

4. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

5. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных, в пределах возложенных на него функций.

6. Организация парольной защиты

6.1. Личные пароли доступа к элементам информационной системы персональных данных создаются пользователем самостоятельно, за исключением временного пароля, который выдает администратор информационной системы персональных данных.

6.2. Пользователь обязан сменить временный пароль, выданный администратором информационной системы персональных данных при первом входе в систему.

Полная плановая смена паролей в информационной системе персональных данных проводится не реже одного раза в 3 месяца.

6.3. Правила формирования пароля:

пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

пароль должен состоять не менее чем из 8 символов.

в пароле должны присутствовать символы трех категорий из числа следующих четырех:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры (от 0 до 9);

символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

запрещается выбирать пароли, которые уже использовались ранее.

6.4. Правила ввода пароля:

ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

6.5. Правила хранения пароля:

запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем;

6.6. Лица, использующие паролирование, обязаны:

четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

своевременно сообщать администратору информационной системы персональных данных об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

7. Правила работы в сетях общего доступа и (или) международного обмена

7.1. Работа в сетях общего доступа и международного обмена (сети Интернет) (далее – Сеть) на элементах информационной системы персональных данных должна проводиться при служебной необходимости.

7.2. При работе в Сети запрещается:

осуществлять работу при отключенных средствах защиты (антивирус и других);

передавать по Сети защищаемую информацию без использования средств шифрования;

запрещается скачивать из Сети программное обеспечение и исполняемые файлы (файлы с расширением exe, dll, msi);

запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие);

запрещается нецелевое использование подключения к Сети.

8. Ответственность

Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

УТВЕРЖДЕН

постановлением администрации

Изобильненского городского
округа Ставропольского края
от 24 апреля 2018 г. № 532

РЕГЛАМЕНТ
порядка действий сотрудников администрации Изобильненского городского округа Ставропольского края при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

Настоящий Регламент разработан на основании и во исполнение Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Целью настоящего Регламента является:

обеспечение прав субъектов персональных данных на доступ к их персональным данным, которые обрабатываются в администрации Изобильненского городского округа Ставропольского края (далее - администрация);

обеспечение прав уполномоченного органа по защите прав субъектов персональных данных на получение информации, необходимой ему для реализации полномочий по защите прав субъектов персональных данных;

упорядочение действий сотрудников администрации при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

Настоящий Регламент распространяется на сотрудников администрации, которые в рамках исполнения своих должностных обязанностей осуществляют прием и регистрацию обращений (запросов) субъектов персональных данных, а также уполномоченного органа по защите прав субъектов персональных данных, осуществляют рассмотрение обращений (запросов), подготовку и направление ответов на них.

Настоящий Регламент подлежит применению исключительно в случаях обращений либо при получении запросов субъектов персональных данных или их законных представителей, а также уполномоченного органа по защите прав субъектов персональных данных в рамках Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1. Общие положения

1.1. Настоящий Регламент использует следующие сокращения:

ПДн – персональные данные;

ИСПДн – информационная система персональных данных.

1.2. Субъект ПДн – это физическое лицо, определенное или определяемое на основании любой относящейся к нему информации.

1.3. Законный представитель субъекта ПДн – это гражданин, который в силу закона выступает во всех учреждениях и организациях от имени и в защиту личных и имущественных прав и законных интересов недееспособных, ограниченно дееспособных граждан, либо дееспособных, но в силу своего физического состояния (по старости, болезни и т. п.) не могущих лично осуществлять свои права и выполнять свои обязанности. В качестве законных представителей выступают родители, усыновители, опекуны и попечители.

1.4. Далее по тексту настоящего Регламента под субъектом ПДн будет подразумеваться также законный представитель субъекта ПДн.

1.5. В соответствии со статьей 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» субъект ПДн имеет право:

на получение сведений о администрации, как операторе ПДн, в т.ч. о месте его нахождения;

на получение сведений о наличии у администрации ПДн, относящихся к соответствующему субъекту персональных данных;

на ознакомление с такими ПДн;

требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

на получение при обращении или при получении запроса информации, касающейся обработки его ПДн, в том числе содержащей:

подтверждение факта обработки персональных данных администрацией, а также цель такой обработки;

способы обработки персональных данных, применяемые администрацией;

сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

перечень обрабатываемых персональных данных и источник их получения;

сроки обработки персональных данных, в том числе сроки их хранения;

сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

1.6. В соответствии со статьей 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» субъект ПДн имеет право отозвать свое согласие на обработку ПДн.

1.7. В соответствии со статьями 14, 20, 21 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» администрация, как оператор ПДн, в случае поступления соответствующего запроса от субъекта ПД обязан:

предоставить субъекту ПДн в доступной форме сведения о наличии его ПДн (при этом указанные сведения не должны содержать ПДн, относящиеся к другим субъектам ПДн);

сообщить субъекту ПДн информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, и другие сведения, право на получение которых субъектом ПДн предусмотрено статьей 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

предоставить возможность ознакомления с ПДн без взимания платы за это;

внести в ПДн необходимые изменения, уничтожить или блокировать соответствующие ПДн по предоставлении субъектом ПДн сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет администрация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

прекратить обработку ПДн и уничтожить их в случае отзыва субъектом ПДн согласия на обработку своих ПДн;

о внесенных изменениях и предпринятых мерах уведомить субъекта ПДн и третьих лиц, которым ПДн этого субъекта были переданы;

уведомить субъекта ПДн об уничтожении ПДн;

1.8. В соответствии с пунктом 3 частью 5 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» право субъекта ПДн на доступ к своим ПДн ограничивается в случае, если предоставление ПДн нарушает конституционные права и свободы других лиц.

2. Действия сотрудников администрации при получении запроса субъекта ПДн

2.1. В соответствии с частью 3 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя согласно приложению1.

2.2. В целях регистрации запросов субъектов ПДн и ответов на такие запросы в администрации осуществляется ведение журнала регистрации запросов субъектов ПДн согласно приложению 2.

2.3. Ответственный за организацию обработки ПДн осуществляет прием и регистрацию запросов субъектов ПДн, а также рассмотрение, подготовку, регистрацию и направление ответов на такие запросы.

2.4. При получении запроса (обращения) физического лица, сотрудник администрации, ответственный за прием и регистрацию входящей корреспонденции в администрации, непосредственно в день получения устанавливает:

2.4.1. Содержит ли запрос фамилию, имя, отчество (последнее при его наличии) гражданина или его законного представителя, номер основного документа, удостоверяющего личность гражданина или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

2.4.2. Содержит ли почтовый адрес, по которому должен быть направлен ответ;

2.4.3. Имеется ли собственноручная подпись, а если запрос направлен в электронной форме, то имеется ли электронная цифровая подпись;

2.4.4.Сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором;

2.4.5. Отвечает ли такой запрос (обращение) требованиям, установленным статьей 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», к запросу субъекта ПДн.

2.5. В случае если при приеме запроса (обращения) физического лица будет установлено, что он содержит в себе все сведения, перечисленные в пункте 2.4. настоящего Регламента то такой запрос подлежит приему и регистрации в журнале регистрации запросов субъектов ПДн в тот же день.

2.6. В случае, если при приеме запроса (обращения) физического лица будет установлено, что он не содержит в себе сведений, перечисленных в пункте 2.4. настоящего Регламента, то такой запрос подлежит приему и ре-

гистрации в порядке, предусмотренном администрацией для приема и регистрации прочей входящей корреспонденции.

2.7. Запросы субъектов ПДн, зарегистрированные в соответствии с пунктом 2.5. настоящего Регламента, в день регистрации подлежат передаче сотруднику (сотрудникам) администрации, указанному (-ным) в пункте 2.3. настоящего Регламента.

2.8. Сотрудники администрации, ответственные за рассмотрение запросов субъектов персональных данных, обязаны рассмотреть запрос субъекта ПДн и подготовить ответ на него в письменной форме в течение десяти рабочих дней с даты получения администрацией указанного запроса.

2.9. В случае если в запросе субъект ПДн изъявил желание ознакомиться со своими ПДн, возможность такого ознакомления должна быть предоставлена субъекту ПДн в течение десяти рабочих дней с даты получения администрацией указанного запроса.

2.10. Письменный ответ на запрос субъекта ПДн должен быть направлен в его адрес заказным письмом с уведомлением о вручении в течение десяти рабочих дней с даты получения администрацией указанного запроса согласно приложению 3.

2.11. Если при рассмотрении запроса субъекта ПДн будет установлено, что предоставление ПДн нарушает конституционные права и свободы других лиц, администрация сообщает ему об отказе в предоставлении информации о ПДн либо таких ПДн, о чем в срок, не превышающий семи рабочих дней со дня получения запроса субъекта ПДн в адрес субъекта ПДн направляется мотивированный ответ в письменной форме, содержащий ссылку на положение пункта 4 части 8 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2.12. Для обработки персональных данных, содержащихся в обращении в письменной форме субъекта ПД, дополнительного согласия не требуется.

3. Действия сотрудников администрации при получении запроса уполномоченного органа по защите прав субъектов персональных данных

3.1. Прием и регистрация запросов уполномоченного органа по защите прав субъектов ПДн осуществляется администрацией в порядке, установленном для приема и регистрации входящей корреспонденции.

3.2. При получении запроса уполномоченного органа по защите прав субъектов ПДн сотрудники администрации, ответственные за прием и регистрацию входящей корреспонденции, в тот же день осуществляют регистрацию такого запроса и передают его сотрудникам указанным в пункте 2.3

3.3. Администрация, в лице сотрудников, указанных в пункте 2.3. настоящего Регламента, сообщает в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, а также направляет истребуемые им документы в течение семи рабочих дней с даты получения такого запроса.

3.4. В случае выявления уполномоченным органом по защите прав субъектов ПДн фактов недостоверности ПДн или неправомерных действий с ними, уточнение, блокирование или уничтожение таких ПДн осуществляется в порядке и сроки, предусмотренные пунктом 4 настоящего Регламента для соответствующих действий (операций) в отношении ПДн.

4. Действия сотрудников администрации при получении требования субъекта ПДн об уточнении своих ПДн, их блокировании или уничтожении; в случае выявления при обращении или по запросу субъекта ПДн фактов недостоверности ПДн или неправомерных действий с ними; в случае отзыва субъектом ПДн согласия на их обработку

4.1. При получении требований субъектов ПДн об уточнении своих ПДн, их блокировании, уничтожении прием и регистрация таких требований осуществляется в порядке, предусмотренном пунктом 2 настоящего Регламента.

4.2. Требования субъектов ПДн в тот же день передаются сотрудникам администрации, указанным в пункте 2.3.

4.3. Полномочные сотрудники администрации вносят в ПДн субъекта необходимые изменения, уничтожают или блокируют соответствующие ПДн по предоставлении субъектом ПДн сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет администрация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

4.4. О внесенных изменениях и предпринятых мерах администрация обязана уведомить субъекта ПДн и третьих лиц, которым ПДн этого субъекта были переданы.

4.5. В случае если факт недостоверности ПДн или неправомерных действий с ними будет выявлен при обращении или по запросу субъекта ПДн администрация обязана осуществить блокирование ПДн, относящихся к соответствующему субъекту ПДн, с момента такого обращения или получения такого запроса на период проверки.

4.6. В случае подтверждения факта недостоверности ПДн администрация на основании документов, представленных субъектом ПДн, или иных необходимых документов обязана уточнить ПДн и снять их блокирование.

4.7. В случае выявления неправомерных действий с ПДн администрация в срок, не превышающий трех рабочих дней с даты такого выявления, обязана устранить допущенные нарушения.

4.8. В случае невозможности устранения допущенных нарушений администрация в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, обязана уничтожить ПДн.

4.9. Об устранении допущенных нарушений или об уничтожении ПДн администрация обязана уведомить субъекта ПДн.

4.10. В случае отзыва субъектом ПДн согласия на обработку своих ПДн администрация обязана прекратить обработку ПДн и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено федеральным законодательством. Об уничтожении ПДн администрация обязан уведомить субъекта ПДн.

Приложение 1

к Регламенту порядка действий сотрудников администрации Изобильненского городского округа Ставропольского края при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных, утвержденному постановлением администрации Изобильненского городского округа Ставропольского края
от 24 апреля 2018 г. № 532

Главе Изобильненского городского округа Ставропольского края
В.И. Козлову
От
паспорт серия номер

(когда и кем выдан)

проживающий по адресу:

Контактный номер телефона:

Руководствуясь статьей 14 Федерального закона «О персональных данных», прошу Вас предоставить мне следующую информацию:

1. Какова цель обработки моих персональных данных в администрации Изобильненского городского округа Ставропольского края;

2. Каковы способы обработки моих персональных данных, применяемые в администрации Изобильненского городского округа Ставропольского края, как оператором персональных данных;

3. Какие лица имеют доступ к моим персональным данным и каким лицам может быть предоставлен такой доступ;

4. Каков перечень обрабатываемых в администрации Изобильненского городского округа Ставропольского края принадлежащих мне персональных данных и каков источник их получения;

5. Каковы сроки обработки моих персональных данных и каковы сроки их хранения;

6. Какие юридические последствия для меня, как для субъекта персональных данных, может повлечь за собой обработка моих персональных данных.

Фамилия И.О. (Подпись) (Дата)

Приложение 2

к Регламенту порядка действий сотрудников администрации Изобильненского городского округа Ставропольского края при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных, утвержденному постановлением администрации Изобильненского городского округа Ставропольского края
от 24 апреля 2018 г. № 532

Администрация Изобильненского городского округа Ставропольского края
Журнал обращений субъектов персональных данных

Фамилия, Имя, Отчество субъекта персональных данных или его законного представителя	Входящий номер, дата обращения субъекта персональных данных	Исходящий номер, дата ответа на запрос субъекта персональных данных

Приложение 3

к Регламенту порядка действий сотрудников администрации Изобильненского городского округа Ставропольского края при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных, утвержденному постановлением администрации Изобильненского городского округа Ставропольского края
от 24 апреля 2018 г. № 532

Исх № От

Фамилия Имя Отчество
Адрес

Уважаемый (ая) _____!

Руководствуясь положениями статей 14, 20 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» сообщаем Вам, что администрация Изобильненского городского округа Ставропольского края обрабатывает Ваши персональные данные.

1. Цель обработки Ваших персональных – реализации полномочий возложенных на орган местного самоуправления федеральным законодательством, законодательством Ставропольского края и нормативно-правовыми актами администрации_____
(указать цель, заранее определенную до начала обработки)

2. Способы обработки Ваших персональных данных – автоматизированная обработка, неавтоматизированная обработка, смешанная обработка.

3. Лица, имеющие доступ к Вашим персональным данным: сотрудники (служащие) администрации Изобильненского городского округа Ставропольского края, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным. Доступ к Вашим персональным данным может быть предоставлен органам, осуществляющим оперативно-розыскную деятельность, органам дознания, следствия, суда.

Перечень обрабатываемых персональных данных: граждане, обратившиеся в администрацию: фамилия, имя, отчество, год рождения, дата рождения, место рождения, адрес, контактные сведения, паспортные данные, семейное положение, состав семьи, степень родства, имущественное положение, доходы, информация о трудовой деятельности, трудоспособность, СНИЛС, состояние здоровья, судимость, сведения о счете в банке, сведения об имуществе.

Срок обработки Ваших персональных данных – до достижения целей обработки.

4. Обработка Ваших персональных данных влечет для Вас в качестве юридических последствий возникновение у Вас прав, присущих субъекту персональных данных и предусмотренных статьей 14 ФЗ «О персональных данных.

С настоящей Инструкцией ознакомлен (на):

Должность	Фамилия Имя Отчество	Дата и подпись

С настоящим Регламентом ознакомлен (на):

Должность	Фамилия Имя Отчество	Дата и подпись