АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ УСТЬ-ЛАБИНСКИЙ РАЙОН

Р А С П О Р Я Ж Е Н И Е

от 26.09.2016 № 289-р

город Усть-Лабинск

Об утверждении внутренних нормативно-правовых актов по защите персональных данных

Для обеспечения безопасности персональных данных при их обработке в администрации муниципального образования Усть-Лабинский район во исполнение требований Федерального закона от 27 июля 2006 года № 152 «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 года № 1119 «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 следующий перечень нормативно-правовых актов:

1.1. Инструкцию системного администратора информационных систем персональных данных по обеспечению безопасности персональных данных в администрации муниципального образования Усть-Лабинский район, (Приложение № 1).

1.2. Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в администрации муниципального образования Усть-Лабинский район (Приложение № 2).

1.3. Инструкцию ответственного за обработку персональных данных в администрации муниципального образования Усть-Лабинский район (Приложение № 3).

1.4. Инструкцию по организации антивирусной защиты в администрации муниципального образования Усть-Лабинский район (Приложение № 4).

1.5. Инструкцию по порядку учета и хранению документов, содержащих персональные данные, в администрации муниципального образования Усть-Лабинский район (Приложение № 5).

1.6. Инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в администрации муниципального образования Усть-Лабинский район (Приложение № 6).

1.7. Инструкцию по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в администрации муниципального образования Усть-Лабинский район (Приложение № 7).

1.8. Инструкцию пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в администрации муниципального образования Усть-Лабинский район (Приложение № 8).

1.9. Положение об обработке персональных данных в администрации муниципального образования Усть-Лабинский район (Приложение № 9).

1.10. Порядок доступа сотрудников администрации муниципального образования Усть-Лабинский район в помещения, где ведётся обработка персональных данных (Приложение № 10).

1.11. Правила работы с обезличенными персональными данными в администрации муниципального образования Усть-Лабинский район (Приложение № 11).

1.12. Регламент порядка действий сотрудников администрации муниципального образования Усть-Лабинский район, при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных (Приложение № 12).

1.13. Инструкцию осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального образования Усть-Лабинский район (Приложение № 13).

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

3. Контроль за выполнением настоящего распоряжения возложить на заместителя главы муниципального образования Усть-Лабинский район В.Г. Ефременко.

4. Распоряжение вступает в силу со дня его подписания.

Глава муниципального образования
Усть-Лабинский район С.В.Батурин

ОБЩИЙ ОТДЕЛ

127091

ПРИЛОЖЕНИЕ № 4
УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Усть-Лабинский район
от 26.09.2016 №289-р

ИНСТРУКЦИЯ
по организации антивирусной защиты в администрации муниципального образования Усть-Лабинский район

1. Общие положения

Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в администрации муниципального образования Усть-Лабинский район (далее - Администрация) и предотвращения возникновения фактов заражения вредоносным программным обеспечением.

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

2. Установка и обновление антивирусных средств

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

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

3. Требования к проведению мероприятий по антивирусной защите

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).

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

Контроль информации на съёмных носителях производится непосредственно перед её использованием.

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.

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

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

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

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.

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

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

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

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

С настоящей Инструкцией по организации антивирусной защиты в администрации муниципального образования Усть-Лабинский район ознакомлен:

Фамилия Имя Отчество	Должность	Дата и подпись

ПРИЛОЖЕНИЕ № 5
УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Усть-Лабинский район
от 26.09.2016 №289-р

ИНСТРУКЦИЯ
по порядку учета и хранению документов, содержащих персональные данные, в администрации муниципального образования Усть-Лабинский район

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 муниципального образования Усть-Лабинский район (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.

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 относится 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, удо-

стоверяющих личность, за исключением случаев, предусмотренных законодательством.

5. Ответственность

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

С настоящей Инструкцией ознакомлен:

Фамилия Имя Отчество	Должность	Дата и подпись

ПРИЛОЖЕНИЕ № 6
УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Усть-Лабинский район
от 26.09.2016 №289-р

ИНСТРУКЦИЯ
по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в администрации муниципального образования Усть-Лабинский район

1. Общие положения

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования средств криптографической защиты информации (СКЗИ) и криптографических ключей, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации в администрации муниципального образования Усть-Лабинский район (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.

2. Обязанности Пользователя

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

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

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

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

2.5. Пользователь обязан немедленно уведомлять Ответственного за обработку персональных данных о компрометации криптографических ключей.

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

3. Порядок обращения со средствами криптографической защиты информации

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

3.2. Все СКЗИ и НКИ должны учитываться в журнале.

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

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

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

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

3.7. 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.

4. Порядок обращения с ключами ЭЦП

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

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

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

4.4. 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.

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

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

5. Запрещается

5.1. Осуществлять несанкционированное и без учётное копирование ключевых данных.

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

5.3. Передавать НКИ третьим лицам.

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

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

5.6. Использование выведенных из действия криптографических ключей.

6. Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

6.1. 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).

6.2. 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.

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

6.4. Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь получает в Удостоверяющем центре новые

ключи ЭЦП.

7. Ответственность Пользователя

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

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

С настоящей Инструкцией по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в администрации муниципального образования Усть-Лабинский район ознакомлен:

Фамилия Имя Отчество	Должность	Дата и подпись

ПРИЛОЖЕНИЕ № 7
УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Усть-Лабинский район
от 26.09.2016 № 289-р

ИНСТРУКЦИЯ

по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в администрации муниципального образования Усть-Лабинский район

1. Общие положения

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

1.4. Действие настоящей Инструкции распространяется на сотрудников администрации муниципального образования Усть-Лабинский район (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 обработке персональ-

ных 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 записанной 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 обработки персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

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 относится 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.

С настоящей Инструкцией по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в администрации муниципального образования Усть-Лабинский район ознакомлен:

Фамилия Имя Отчество	Должность	Дата и подпись

ПРИЛОЖЕНИЕ № 8
УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Усть-Лабинский район
от 26.08.2016 № 289-р

ИНСТРУКЦИЯ

пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в администрации муниципального образования Усть-Лабинский район

1. Общие положения

Пользователь информационной системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных в информационных системах персональных данных в администрации муниципального образования Усть-Лабинский район (далее – Администрация).

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.

Пользователь несет персональную ответственность за свои действия.

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

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 (Раздел 3).

Соблюдать правила при работе в сетях общего доступа и международно-

го обмена – Интернет (Раздел 4).

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).

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.

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

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.

Несанкционированно 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.

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>

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

3. Организация парольной защиты

Личные пароли доступа к элементам информационной системы персо-

нальных данных создаются пользователем самостоятельно, за исключением временного пароля, который выдает Администратор информационной системы персональных данных.

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.

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.

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.).

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.

Лица, использующие паролирование, обязаны:

Четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию.

Своевременно сообщать Администратору информационной системы пер-

сональных данных об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

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

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

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.

5. Ответственность

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

С настоящей Инструкцией пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в администрации муниципального образования Усть-Лабинский район ознакомлен:

Фамилия Имя Отчество	Должность	Дата и подпись

ПРИЛОЖЕНИЕ № 9
УТВЕРЖДЕНО
распоряжением администрации
муниципального образования
Усть-Лабинский район
от 26.09.2016 № 289-р

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в администрации муниципального образования Усть-Лабинский район

1. Общие положения

Положение об обработке и защите персональных данных в администрации муниципального образования Усть-Лабинский район (далее - Положение) определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в администрации муниципального образования Усть-Лабинский район (далее - Администрация).

Настоящее Положение определяет политику Администрации как оператора, осуществляющего обработку персональных данных и определяющего цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Настоящее Положение разработано в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 25 декабря 2008 года № 273-ФЗ «О противодействии коррупции», Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федеральным законом от 2 сентября 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Субъектами персональных данных являются работники Администрации, граждане, претендующие на замещение вакантных должностей в Администрации, а также члены их семей; граждане запросы и обращения которых рассматриваются в связи с предоставлением муниципальных услуг, исполнением муниципальных функций и рассмотрением обращений граждан; дети, оставшиеся без попечения родителей, усыновленные дети, их родители, опекуны и другие законные представители; работники образовательных учреждений, учащиеся, воспитанники и их родители (законные представители); несовершеннолетние, находящимся в социально опасном положении.

Обработка персональных данных в Администрации выполняется с использованием средств автоматизации и без использования таких средств и включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Обработка персональных данных в Администрации осуществляется с соблюдением принципов и условий, предусмотренных настоящим Положением и законодательством Российской Федерации в области персональных данных.

2. Условия и порядок обработки персональных данных в связи с реализацией служебных или трудовых отношений

Персональные данные муниципальных служащих Администрации и работников Администрации (далее – сотрудники Администрации), граждан, претендующих на замещение должностей сотрудников Администрации, обрабатываются в целях обеспечения кадровой работы, в том числе в целях содействия в прохождении муниципальной службы, содействия в выполнении осуществляемой работы, формирования кадрового резерва, обучения и должностного роста, учета результатов исполнения должностных обязанностей, обеспечения личной безопасности сотрудников, включая членов их семей, обеспечения установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества, а также в целях противодействия коррупции.

Состав обрабатываемых персональных данных определяется в соответствии с перечнем персональных данных, обрабатываемых в администрации муниципального образования Усть-Лабинский район (Приложение №1 к данному Положению).

Обработка персональных данных осуществляется при условии получения письменного согласия субъекта персональных данных, если иное не установлено Федеральным законом «О персональных данных» (Приложение №4 к данному Положению).

Обработка персональных данных сотрудников Администрации, граждан, претендующих на замещение должностей сотрудников Администрации, осуществляется сектором по кадровым вопросам управления по организационно

правовым вопросам и взаимодействию с органами местного самоуправления администрации муниципального образования Усть-Лабинский район (далее – Сектор по кадровым вопросам) и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных сотрудников Администрации, граждан, претендующих на замещение должностей сотрудников Администрации, осуществляется путем:

1) получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые в Сектор по кадровым вопросам);

2) копирования оригиналов документов;

3) внесения сведений в учётные формы (на бумажных и электронных носителях);

4) формирования персональных данных в ходе кадровой и бухгалтерской работы;

5) внесения персональных данных в информационную систему персональных данных сотрудников Администрации, используемую Сектором по кадровым вопросам.

Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от сотрудников Администрации, граждан, претендующих на замещение должностей сотрудников Администрации.

Запрещается получать, обрабатывать и приобщать к личному делу сотрудников Администрации, граждан, претендующих на замещение должностей сотрудников Администрации, персональные данные, не предусмотренные пунктом 2.2 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

При сборе персональных данных сотрудник Сектора по кадровым вопросам, осуществляющий сбор (получение) персональных данных непосредственно от сотрудников Администрации, граждан, претендующих на замещение должностей сотрудников Администрации, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

В случае возникновения необходимости получения персональных данных субъекта персональных данных у третьей стороны следует заранее известить об этом субъекта персональных данных, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных.

Передача (распространение, предоставление) и использование персональных данных сотрудников Администрации, граждан, претендующих на замеще-

ние должностей сотрудников Администрации, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

3. Условия и порядок обработки персональных данных субъектов в связи с предоставлением муниципальных услуг и исполнением муниципальных функций, рассмотрения обращений граждан

В Администрации обработка персональных данных физических лиц осуществляется в соответствии с административными регламентами предоставления муниципальных услуг и исполнения муниципальных функций, порядком работы с обращениями граждан в администрации муниципального образования Усть-Лабинский район, утвержденными постановлениями администрации муниципального образования Усть-Лабинский район.

Персональные данные граждан, обратившихся в Администрацию лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением заявителей о результатах рассмотрения.

Состав обрабатываемых персональных данных в рамках рассмотрения обращений граждан и предоставления муниципальных услуг и исполнения муниципальных функций определяется в соответствии с перечнем персональных данных, обрабатываемых в администрации муниципального образования Усть-Лабинский район (Приложение № 1 к данному Положению).

Обработка персональных данных, необходимых в связи с предоставлением муниципальных услуг и исполнением муниципальных функций, осуществляется без согласия субъектов персональных данных в соответствии с пунктом 4 части 1 статьи 6 Федерального закона «О персональных данных», Федеральным законом «Об организации предоставления государственных и муниципальных услуг».

Обработка персональных данных, необходимых в связи с предоставлением муниципальных услуг и исполнением муниципальных функций, рассмотрением обращений граждан, осуществляется управлениями, отделами и секторами Администрации, предоставляющими соответствующие муниципальные услуги и (или) исполняющими муниципальные функции, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, обратившихся в Администрацию для получения муниципальной услуги, в целях исполнения муниципальной функции или с обращением, осуществляется путем:

1) получения оригиналов необходимых документов (заявление);
2) заверения копий документов;