Администрация
муниципального образования
«Можгинский район»

«Можга ёрос»
муниципал кылдытэтлэн
Администрациез

РАСПОРЯЖЕНИЕ

от «20» ноября 2018 года **№ 284-р**

О мерах по защите персональных данных
Администрации муниципального образования «Можгинский район»

В соответствии с пунктом 1 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», в целях организации системы мер обеспечения защиты персональных данных,

1. Утвердить прилагаемые:
- инструкцию пользователя информационной системы персональных данных Администрации муниципального образования «Можгинский район»;
- инструкцию администратора по обеспечению безопасности персональных данных при их обработке в информационных системах Администрации муниципального образования «Можгинский район»;
- инструкцию по организации антивирусной защиты в Администрации муниципального образования «Можгинский район».

2. Контроль за выполнением данного распоряжения возложить на руководителя аппарата Администрации района – начальника Управления документационного обеспечения Городилову Н. П.

Глава муниципального образования
«Можгинский район» А. Г. Васильев

УТВЕРЖДЕНА
распоряжением Администрации
муниципального образования
«Можгинский район»
от 20.11.2018г № 284-р

Инструкция администратора по обеспечению безопасности персональных данных при их обработке в информационных системах Администрации муниципального образования «Можгинский район»

I. Общие положения

1. Инструкция администратора по обеспечению безопасности персональных данных при их обработке в информационных системах Администрации муниципального образования «Можгинский район» (далее - ответственный за безопасность ПДн в ИСПДн) по поддержанию уровня защиты локальной вычислительной сети разработана с учётом требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и других нормативных правовых актов (далее - НПА) по защите информации от несанкционированного доступа (далее - НСД).

Целью администрирования локальной вычислительной сети (далее - ЛВС) является поддержка уровня защиты информации ЛВС и информационных ресурсов Администрации муниципального образования «Можгинский район» (далее – Администрация района).

2. Инструкция регулирует отношения между ответственным за безопасность ПДн в ИСПДн, пользователями и разработчиками, возникающие при:

- эксплуатации и развитии ЛВС и информационных ресурсов;
- формировании и использовании данных, сообщений, баз данных, информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления пользователю документированной информации;
- при создании, внедрении и эксплуатации новых информационных технологий.

3. Цели администрирования ЛВС достигаются обеспечением и поддержкой в ЛВС:

- подсистем управления доступом, регистрации и учёта, обеспечения целостности программно-аппаратной среды, хранимой, обрабатываемой и передаваемой по каналам связи информации;
- доступности информации (устойчивое функционирование ЛВС и ее подсистем);
- конфиденциальности хранимой, обрабатываемой и передаваемой по каналам связи информации.

4. Защита ЛВС и информационных ресурсов представляет собой комплекс организационных и технических мероприятий, направленных на исключение или существенное затруднение противоправных действий в отношении ресурсов ЛВС и информационных ресурсов. Мероприятия по защите ЛВС и информационных ресурсов от НСД являются составной частью комплекса организационных и технических мероприятий, направленных на защиту персональных данных в информационной системе.

5. Ответственный за безопасность ПДн в ИСПДн назначается распоряжением Администрации района и является ответственным должностным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ЛВС и ее ресурсов на этапах эксплуатации и модернизации.

6. Ответственный за безопасность ПДн в ИСПДн руководствуется в своей практической деятельности положениями федеральных законов, правовых актов Российской Федерации, Удмуртской Республики, правовыми актами Администрации

района, регламентирующими работу ответственного за безопасность персональных данных.

7. Ответственный за безопасность ПДн в ИСПДн должен иметь специальное автоматизированное рабочее место (далее - АРМ), размещённое в отдельном помещении и функционирующее постоянно при включении сети, а также личный сейф (или железный шкаф) и печать.

8. Ответственный за безопасность ПДн в ИСПДн несёт ответственность в соответствии с действующим законодательством Российской Федерации за разглашение защищаемой информации, соблюдение установленного режима защиты персональных данных, ставших известными в связи с исполнением служебных обязанностей.

9. Требования ответственного за безопасность ПДн в ИСПДн, связанные с выполнением им своих функций, обязательны для исполнения всеми пользователями ЛВС и информационных ресурсов.

10. Настоящая Инструкция не регламентирует вопросы физической защиты и охраны зданий и помещений, в которых расположена ЛВС, вопросы обеспечения физической целостности компонентов ЛВС, защиты от стихийных бедствий (пожаров, наводнений и др.), сбоев в системе энергоснабжения, а также меры обеспечения безопасности персонала и меры, принимаемые при возникновении в ЛВС нештатных ситуаций.

II. Права и обязанности ответственного за безопасность ПДн в ИСПДн

11. Ответственный за безопасность ПДн в ИСПДн имеет право:

- отключать от сети пользователей, осуществивших НСД к защищаемым информационным ресурсам или нарушивших другие требования по безопасности информации;
- участвовать в любых проверках ЛВС и состояния информационных ресурсов;
- запрещать устанавливать на серверах и рабочих станциях ЛВС нештатное программное и аппаратное обеспечение.

12. Ответственный за безопасность ПДн в ИСПДн обязан:

- знать в совершенстве применяемые информационные технологии;
- участвовать в контрольных и тестовых испытаниях и проверках ЛВС и состояния информационных ресурсов;
- знать ответственных лиц в каждом структурном подразделении Администрации района и их права доступа по обработке, хранению и передаче защищаемой информации;
- вести контроль за процессом резервирования и дублирования важных ресурсов ЛВС и информационных ресурсов;
- участвовать в приёмке и тестировании новых программных средств;
- уточнять в установленном порядке обязанности пользователей ЛВС по поддержанию уровня защиты ЛВС;
- вносить предложения по совершенствованию уровня защиты ЛВС и информационных ресурсов;
- анализировать данные журнала учёта работы ЛВС с целью выявления возможных нарушений требований защиты;
- оценивать возможность и последствия внесения изменений в состав ЛВС с учётом требований НПА по защите, подготавливать свои предложения;
- обеспечить доступ к защищаемой информации пользователям ЛВС согласно должностного регламента;
- запрещать и немедленно блокировать попытки изменения программно -аппаратной среды ЛВС без согласования порядка ввода новых (отремонтированных) технических и программных средств и средств защиты ЛВС;
- запрещать и немедленно блокировать применение пользователям сети программ, с помощью которых возможны факты НСД к ресурсам ЛВС и информационных ресурсов;
- незамедлительно докладывать руководству обо всех попытках нарушения защиты ЛВС и информационных ресурсов;

- анализировать состояние защиты ЛВС и её отдельных подсистем;
- контролировать физическую сохранность средств и оборудования ЛВС;
- контролировать состояние средств и систем защиты и их параметры и критерии;
- контролировать правильность применения пользователями средств защиты;
- оказывать помощь пользователям в части применения средств защиты от НСД и других средств защиты, входящих в состав ЛВС;
- не допускать установку, использование, хранение и размножение в ЛВС программных средств, не связанных с выполнением функциональных задач;
- своевременно анализировать журнал учёта событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;
- в период профилактических работ на рабочих станциях и серверах ЛВС снимать при необходимости средства защиты ЛВС с эксплуатации с обязательным обеспечением сохранности информации;
- не допускать к работе на рабочих станциях и серверах ЛВС посторонних лиц;
- осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ЛВС;
- периодически предоставлять в сектор программного обеспечения ГО и ЧС отчёт о состоянии защиты ЛВС, о нештатных ситуациях на объектах ЛВС и допущенных пользователями нарушениях установленных требований по защите информации.

13. Ответственному за безопасность ПДн в ИСПДн запрещается: оставлять свою рабочую станцию без контроля в рабочем состоянии; фиксировать учётные данные пользователя (пароли, идентификаторы, ключи и др.) на твёрдых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя.

14. Ответственный за безопасность ПДн в ИСПДн должен четко знать нарушения (противоправные действия) в отношении ЛВС и её подсистем, последствия которых:

- невыполнение пользователями ЛВС требований или норм организационно-распорядительных документов по работе и по защите в информационной сфере, в результате чего имеется реальная возможность противоправных действий в отношении ЛВС и информационных ресурсов.

15. Ответственный за безопасность ПДн в ИСПДн должен поддерживать защиту ЛВС и информационных ресурсов от несанкционированного доступа к информации.

16. Ответственный за безопасность ПДн в ИСПДн несёт персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ЛВС, состояние и поддержание установленного уровня защиты ЛВС.

III. Требования к рабочей станции и инструментальным средствам ответственного за безопасность ПДн в ИСПДн

17. Рабочая станция ответственного за безопасность ПДн в ИСПДн должна представлять собой специально выделенную ПЭВМ, которая является пунктом управления и контроля уровня защиты ЛВС и ее ресурсов.

18. Рабочая станция ответственного за безопасность ПДн в ИСПДн размещается в отдельном помещении, доступ в которое имеют только должностные лица, определённые распоряжением Администрации муниципального образования «Можгинский район».

19. Инструментальные средства, установленные на рабочей станции ответственного за безопасность ПДн в ИСПДн (программные, программно-аппаратные, аппаратные), должны позволять эффективно решать задачи, поставленные перед ним.

С настоящей инструкцией ознакомлен:

_____ _____ «____»_____ 20__ г.
ФИО подпись

_____ _____ «____»_____ 20__ г.
ФИО подпись

УТВЕРЖДЕНА
распоряжением Администрации
муниципального образования
«Можгинский район»
от 20.11.2018г. № 284-р

Инструкция пользователя информационной системы персональных данных Администрации муниципального образования «Можгинский район»

I. Общие положения

1. Пользователь информационной системы персональных данных (далее - пользователь ИСПДн) осуществляет обработку персональных данных в информационной системе персональных данных (далее - ИСПДн) Администрации муниципального образования «Можгинский район» (далее – Администрация района).
2. Пользователем ИСПДн является каждый работник Администрации района, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
3. Пользователь ИСПДн несёт персональную ответственность за свои действия.
4. Пользователь ИСПДн в своей работе руководствуется настоящей Инструкцией, положениями федеральных законов, правовых и иных актов Российской Федерации, Удмуртской Республики, правовыми актами Администрации района, регламентирующими работу с персональными данными.
5. Методическое руководство работой пользователя осуществляется администратором по обеспечению безопасности персональных данных при их обработке в информационных системах Администрации района (далее -ответственный за безопасность ПДн в ИСПДн).

II. Должностные обязанности

6. Пользователь ИСПДн обязан:
- знать и выполнять требования настоящей Инструкции и других внутренних документов, регламентирующих порядок действий по защите персональных данных;
- выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностным регламентом;
- знать и соблюдать установленные в Администрации района требования по режиму обработки персональных данных, учёту, хранению и пересылке носителей информации, обеспечению безопасности персональных данных;
- соблюдать требования парольной защиты;
- соблюдать правила при работе в сетях общего доступа и (или) международного обмена (Интернет и других);
- экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нём информацией посторонними лицами, шторы на оконных проёмах должны быть завешаны (жалюзи закрыты);
- обо всех выявленных нарушениях, связанных с информационной безопасностью Администрации района, а так же для получений консультаций по вопросам информационной безопасности, обращаться к ответственному за безопасность ПДн в ИСПДн;

- при отсутствии визуального контроля за рабочей станцией доступ к компьютеру блокировать путём нажатия одновременно комбинации 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, в пределах возложенных на него функций.

7. Пользователям ИСПДн запрещается:

- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения своего руководителя;
- самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции 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 ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за безопасность ПДн в ИСПДн.

Ш.Организация парольной защиты

8. Личные пароли доступа к элементам ИСПДн выдаются пользователям ответственным за безопасность ПДн в ИСПДн или создаются самостоятельно.

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

10. Правила формирования пароля:

- пароль не может содержать имя учётной записи пользователя ИСПДн или какую-либо его часть;
- пароль должен состоять не менее чем из 8 символов;
- в пароле должны присутствовать символы трёх категорий из числа следующих четырёх:
- 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, !,$,#,%).

11. Запрещается:

- использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же 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;
- использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567);
- выбирать пароли, которые уже использовались ранее.

12. 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.

13. Правила хранение 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.

14. Лица, использующие пародирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции;

- своевременно сообщать ответственному за безопасность ПДн в ИСПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

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

15. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИСПДн должна проводиться при служебной необходимости.

16. 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 другие файлы;

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

- запрещается нецелевое использование подключения к Сети.

17. Настоящая Инструкция доводится до пользователей под роспись по форме согласно приложению.

Приложение
к Инструкции пользователя
информационной системы
персональных данных Администрации
муниципального образования
«Можгинский район»

Лист ознакомления

С инструкцией ознакомлен(ы):

№ п/п	Ф.И.О.	Дата ознакомления	Роспись в ознакомлении
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			

УТВЕРЖДЕНА
Распоряжением Администрации
муниципального образования
«Можгинский район»
от 20.11.2018г №284-р

Инструкция по организации антивирусной защиты в Администрации муниципального образования «Можгинский район»

I. Общие положения

1. Настоящая Инструкция определяет требования к организации защиты объектов вычислительной техники (далее - ОВТ) автоматизированной системы (далее - АС) Администрации муниципального образования «Можгинский район» (далее – Администрация района) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и работников в Администрации района, эксплуатирующих и сопровождающих АС Администрации района, за их выполнение.

2. К использованию в Администрации района допускаются только лицензионные и сертифицированные антивирусные средства.

3. Установка и настройка параметров средств антивирусного контроля на компьютерах, серверах локальной вычислительной сети (далее - ЛВС) осуществляется ответственным по обеспечению информационной безопасности в Администрации района.

4. Централизованное управление и мониторинг средств антивирусного контроля ОВТ осуществляется ответственным по обеспечению информационной безопасности в Администрации района.

II. Применение средств антивирусного контроля

5. В начале работы при загрузке компьютера в обязательном порядке должна быть запущена антивирусная программа.

6. Обновление антивирусных средств должно происходить в автоматическом режиме при загрузке ОВТ. Допускается работа антивируса с обновлениями не старше 72 часов.

7. Антивирусный контроль всех дисков и файлов ОВТ должен проводиться еженедельно в автоматическом режиме.

8. Внеочередной антивирусный контроль всех дисков и файлов ОВТ должен выполняться:

- непосредственно после установки (изменения) программного обеспечения на ОВТ;

- 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.).

9. Ежеквартально для каждого компьютера (в том числе для серверов ЛВС) должен проводиться антивирусный контроль всех дисков и файлов автоматизированных рабочих мест (далее - АРМ).

10. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съёмных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после её приёма на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистой" (не заражённой вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации,

обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съёмный носитель).

11. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в полгода пользователем АРМ.

12. Установка (изменение) системного и прикладного программного обеспечения осуществляется системным администратором ЛВС.

13. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено ответственным по обеспечению информационной безопасности в Администрации района. Непосредственно после установки (изменения) программного обеспечения компьютера ЛВС, должна быть выполнена антивирусная проверка:

- на защищаемых серверах и АРМ - ответственным за обеспечение информационной безопасности;

- на других серверах и АРМ АС Администрации района, не требующих защиты, лицом, установившим (изменившим) программное обеспечение, в присутствии и под контролем ответственного по обеспечению информационной безопасности в Администрации района.

III. Применение средств антивирусного контроля при возникновении компьютерного вируса

14. 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.) работник Администрации района самостоятельно или вместе с ответственным, за обеспечение информационной безопасности должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлекаются ответственные по обеспечению информационной безопасности в Администрации района для определения ими факта наличия или отсутствия компьютерного вируса.

15. В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов работники Администрации района обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения заражённых вирусом файлов руководителя структурного подразделения Администрации района и ответственного за обеспечение информационной безопасности, владельца заражённых файлов, а также смежные структурные подразделения Администрации района, использующие эти файлы в работе;

- совместно с владельцем заражённых вирусом файлов провести анализ необходимости дальнейшего их использования;

- провести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь ответственного по обеспечению информационной безопасности в Администрации района);

- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить заражённый вирусом файл на гибком магнитном диске ответственному по обеспечению информационной безопасности в Администрации района для дальнейшей передачи его в организацию, с которой заключён договор на антивирусную поддержку;

- по факту обнаружения заражённых вирусом файлов необходимо указать предполагаемый источник (отправителя, владельца и т.д.) заражённого файла, тип заражённого файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

IV. Ответственность

17. Ответственность за организацию антивирусного контроля в Администрации района, в соответствии с требованиями настоящей Инструкции, возлагается на ответственного по обеспечению информационной безопасности в Администрации района

18. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение информационной безопасности и всех работников, являющихся пользователями АС Администрации района.

17. Периодический контроль за состоянием антивирусной защиты в АС Администрации района, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции работниками Администрации района осуществляется ответственным по обеспечению информационной безопасности в Администрации района.