Российская Федерация
Костромская область
АДМИНИСТРАЦИЯ СОЛИГАЛИЧСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

ПОСТАНОВЛЕНИЕ

от 27 марта 2024 года № 367

г. Солигалич

Об утверждении документов, определяющих политику в отношении обработки персональных данных в администрации Солигаличского муниципального округа Костромской области

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлениями Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ними нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами», статьей 6 Устава муниципального образования Солигаличский муниципальный район Костромской области и в целях совершенствования системы защиты персональных данных работников администрации Солигаличского муниципального округа Костромской области,

администрация Солигаличского муниципального округа Костромской области ПОСТАНОВЛЯЕТ:

1. Утвердить:

1.1. Правила обработки персональных данных в администрации Солигаличского муниципального округа Костромской области (приложение №1);

1.2. Типовую форму согласия на обработку персональных данных (приложение №2);

1.3. Форму согласия на получение персональных данных у третьей стороны (приложение №3);

1.4. Заявление об отзыве согласия на обработку персональных данных (приложение №4);

1.5. Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (приложение №5);

1.6. Типовое обязательство муниципального служащего администрации Солигаличского муниципального округа Костромской области, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (приложение №6);

1.7. Форму листа ознакомления муниципального служащего (работника) администрации Солигаличского муниципального округа Костромской области, непосредственно осуществляющего обработку персональных данных, с положениями законодательства о персональных данных (приложение №7);

1.8. Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации Солигаличского муниципального округа Костромской области (приложение №8);

1.9. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Солигаличского муниципального округа Костромской области (приложение №9);

1.10. Правила работы с обезличенными данными в администрации Солигаличского муниципального округа Костромской области в случае обезличивания персональных данных (приложение №10);

1.11. Перечень персональных данных, обрабатываемых в администрации Солигаличского муниципального округа Костромской области, в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций (приложение №11);

1.12.Перечень должностей в администрации Солигаличского муниципального округа Костромской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, в том числе работу с информационными системами, базами данных, содержащими персональные данные (приложение №12);

1.13. Перечень должностей в администрации Солигаличского муниципального округа Костромской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных (приложение №13);

1.14. Должностную инструкцию ответственного за организацию обработки персональных данных в администрации Солигаличского муниципального округа (приложение №14);

1.15. Порядок доступа в помещения, в которых ведется обработка персональных данных (приложение №15);

1.16. Положение об экспертной комиссии администрации Солигаличского муниципального округа Костромской области (приложение №16);

1.17. Положение об обработке конфиденциальной информации в администрации Солигаличского муниципального округа Костромской области (приложение №17);

1.18. Перечень информационных систем персональных данных, используемых в администрации Солигаличского муниципального округа Костромской области (приложение №18);

1.19. Правила работы с информационными системами администрации Солигаличского муниципального округа Костромской области (приложение №19).

2. Руководителям структурных подразделений администрации муниципального округа с правом юридического лица утвердить (актуализировать):

2.1. перечень информационных систем персональных данных, используемых в структурном подразделении администрации муниципального округа;

2.2. перечень персональных данных, обрабатываемых в структурном подразделении администрации муниципального округа в связи с оказанием муниципальных услуг и осуществлением муниципальных функций;

2.3. перечень должностей работников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

2.4. перечень должностей работников, ответственных за осуществление обработки персональных данных либо осуществление доступа к персональным данным;

2.5. ответственное лицо за организацию обработки персональных данных.

3. Назначить лицом, ответственным за организацию обработки персональных данных в администрации Солигаличского муниципального округа Костромской области управляющего делами администрации Солигаличского муниципального округа Костромской области.

4. Отменить постановления администрации Солигаличского муниципального района Костромской области:

от 03 мая 2018 года № 308 «Об утверждении документов, определяющих политику в отношении обработки персональных данных в администрации Солигаличского муниципального района Костромской области»;

от 27 декабря 2021 года № 1146 «О внесении изменений в постановление администрации Солигаличского муниципального района Костромской области от 03 мая 2018 года № 308 «Об

утверждении документов, определяющих политику в отношении обработки персональных данных в администрации Солигаличского муниципального округа Костромской области»

5. Настоящее постановление вступает со дня официального опубликования в информационном бюллетене «Вестник».

Глава Солигаличского
муниципального округа
Костромской области А.А.Вакуров

Приложение 1 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Правила обработки персональных данных
в администрации Солигаличского муниципального округа Костромской области

I. Общие положения

1. Настоящие Правила в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых 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 «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» регулируют отношения, связанные с порядком приема, учета, сбора, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным.

2. В настоящих Правилах используются термины и определения, установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

3. Принципы обработки персональных данных:

а) обработка персональных данных должна осуществляться на законной и справедливой основе;

б) обработка персональных данных должна ограничиваться достижением конкретных, определенных настоящими Правилами целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

в) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

г) обработке подлежат только персональные данные, которые отвечают целям их обработки;

д) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

е) при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Должностные лица администрации муниципального округа должны принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

ж) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством.

4. Цели обработки персональных данных в администрации Солигаличского муниципального округа Костромской области (далее Администрация):

а) удовлетворения нужд граждан в соответствии с полномочиями Администрации;

б) предоставление муниципальных услуг;

в) правовое закрепление принципов, касающихся обработки персональных данных, порядка хранения и использования в администрации муниципального округа.

5. Персональные данные следует получать лично у субъекта персональных данных, если иное не предусмотрено федеральным законом.

6. Глава муниципального округа, руководитель структурного подразделения Администрации с правом юридического лица соответственно назначает должностное лицо, ответственное за организацию обработки персональных данных, и определяет лиц, уполномоченных на обработку персональных данных, обеспечивающих обработку персональных данных в соответствии с требованиями законодательства и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

7. Обработка персональных данных осуществляется с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие субъекта персональных данных на обработку его персональных данных должно отвечать требованиям, определенным статьей 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

8. Обработка персональных данных допускается в следующих случаях:

а) обработка персональных данных необходима для достижения целей предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

б) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

в) обработка персональных данных необходима для предоставления муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг";

г) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

д) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

е) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

ж) обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

з) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

и) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

9. Гражданин при поступлении на муниципальную службу, в случае если в круг его должностных обязанностей будет входить непосредственное осуществление обработки персональных данных, должен ознакомиться с положениями законодательства Российской Федерации о персональных данных и заполнить форму листа ознакомления.

10. Должностное лицо, ответственное за обработку персональных данных в Администрации, в случае расторжения с ним трудового договора обязуется прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, о чем подписывает соответствующее обязательство при поступлении на муниципальную службу.

11. При сборе персональных данных уполномоченные должностные лица Администрации обязаны предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

12. При обработке персональных данных уполномоченные должностные лица в Администрации обязаны соблюдать следующие требования:

а) обработка персональных данных должна осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;

б) запрещается получать, обрабатывать и приобщать к личному делу субъекта персональных данных персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах субъекта персональных данных;

в) в случае выявления неполных, неточных или неактуальных персональных данных в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица администрации муниципального округа обязаны внести в них необходимые изменения с уведомлением субъекта персональных данных или его представителя;

г) в случае представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные должностные лица в срок, не превышающий семи рабочих дней со дня получения таких сведений, обязаны уничтожить такие персональные данные с уведомлением субъекта персональных данных или его представителя;

д) в случае выявления недостоверных персональных данных или неправомерных действий с ними должностных лиц, при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных, уполномоченные должностные лица обязаны осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки;

е) в случае подтверждения факта недостоверности персональных данных уполномоченные должностные лица на основании документов, представленных субъектом персональных данных, или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование;

ж) в случае выявления неправомерных действий с персональными данными уполномоченные должностные лица в срок, не превышающий трех рабочих дней с даты такого выявления, обязаны устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений, уполномоченные должностные лица в срок, не превышающий десяти рабочих дней с даты выявления неправомерности действий с персональными данными, обязаны уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных уполномоченные должностные лица обязаны уведомить субъекта персональных данных, или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган;

з) в случае отзыва субъектом персональных данных согласия на обработку его персональных данных уполномоченные должностные лица обязаны прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва;

и) хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных, сроком не больше, чем этого требуют цели их обработки, а также они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

13. При передаче персональных данных уполномоченные должностные лица должны соблюдать следующие требования:

а) не сообщать персональные данные третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, установленных федеральными законами;

б) разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

14. Сроки обработки и хранения персональных данных, порядок их уничтожения при достижении целей обработки или при наступлении иных законных оснований определяются нормами законодательства Российской Федерации в сфере муниципальной службы, трудового законодательства, законодательства об архивном деле.

15. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных федеральным законом.

16. Обработка персональных данных в Администрации ограничивается достижением конкретных, заранее определенных и законных целей. Содержание и объём обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки. Обработка персональных данных, несовместимая с целями сбора персональных данных, не допускается.

17.Трансграничная передача персональных данных не осуществляется.

II. Условия и порядок обработки персональных данных по субъектам персональных данных

1. Субъектами персональных данных являются:

а) муниципальные служащие;

б) родственники муниципальных служащих;

в) работники, замещающие должности, не являющиеся должностями муниципальной службы;

г) родственники работников, замещающих должности, не являющиеся должностями муниципальной службы;

д) граждане, включенные в кадровый резерв;

е) граждане, претендующие на замещение вакантных должностей муниципальной службы;

ж) родственники граждан, претендующих на замещение вакантных должности муниципальной службы;

з) руководители муниципальных предприятий;

и) руководители муниципальных учреждений;

к) родственники руководителей муниципальных предприятий и учреждений;

л) физические лица в связи с предоставлением муниципальной услуги и исполнением муниципальных функций и полномочий;

м) физические лица, обратившиеся в администрацию муниципального округа;

н) представители юридических лиц, обратившихся в администрацию муниципального округа;

о) физические лица, персональные данные которых получены в ходе контрольной деятельности;

п) физические лица, в отношении которых составляются протоколы об административных правонарушениях и рассматриваются дела об административных правонарушениях;

р) уволенные сотрудники.

2. Условия и порядок обработки персональных данных муниципальных служащих

2.1. Персональные данные муниципальных служащих администрации муниципального округа, (далее - муниципальные служащие) обрабатываются в целях обеспечения кадровой работы, в том числе в целях содействия муниципальным служащим в прохождении муниципальной службы, формирования кадрового резерва муниципальной службы, обучения и должностного роста, учета результатов исполнения муниципальными служащими должностных

обязанностей, обеспечения личной безопасности муниципальных служащих и членов их семьи, обеспечения муниципальным служащим установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества, в целях организации информационно-технического обеспечения администрации муниципального округа, а также в целях противодействия коррупции.

2.2. В целях, указанных в пункте 2.1 настоящего раздела, обрабатываются следующие категории персональных данных муниципальных служащих:

2.2.1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

2.2.2. число, месяц, год рождения;

2.2.3. место рождения;

2.2.4. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

2.2.5. пол;

2.2.6. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

2.2.7. адрес места жительства (адрес регистрации, фактического проживания);

2.2.8. номер контактного телефона или сведения о других способах связи;

2.2.9. реквизиты страхового свидетельства государственного пенсионного страхования;

2.2.10. идентификационный номер налогоплательщика;

2.2.11. реквизиты страхового медицинского полиса обязательного медицинского страхования;

2.2.12. реквизиты свидетельства государственной регистрации актов гражданского состояния;

2.2.13. серия, номер заграничного паспорта, наименование органа, выдавшего его, дата выдачи;

2.2.14. семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

2.2.15. сведения о трудовой деятельности;

2.2.16. сведения о воинском учете и реквизиты документов воинского учета;

2.2.17. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

2.2.18. сведения об ученой степени;

2.2.19. информация о владении иностранными языками, степень владения;

2.2.20. медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению;

2.2.21. фотография;

2.2.22. сведения о прохождении государственной гражданской службы, муниципальной службы в том числе: дата, основания поступления на государственную гражданскую служб, муниципальную службу и назначения на должность государственной гражданской службы, муниципальной службы, дата, основания назначения, перевода, перемещения на иную должность государственной гражданской службы, муниципальной службы, наименование замещаемых должностей государственной гражданской службы, муниципальной службы с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности государственной гражданской службы, муниципальной службы, а также сведения о прежнем месте работы;

2.2.23. информация, содержащаяся в служебном (муниципальном) контракте (трудовом договоре), дополнительных соглашениях к ним;

2.2.24. сведения, указанные в свидетельствах государственной регистрации актов гражданского состояния;

2.2.25. сведения о беременности;

2.2.26. сведения об инвалидности;

2.2.27. сведения о пребывании за границей;

2.2.28. информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы);

2.2.28. сведения о родственниках, проживающих за границей и (или) оформивших документы для выезда на постоянное место жительства в другое государство;

2.2.29. сведения о наличии или отсутствии судимости;

2.2.30. информация об оформленных допусках к государственной тайне;

2.2.31. государственные награды, иные награды и знаки отличия;

2.2.32. сведения о профессиональной переподготовке и (или) повышении квалификации;

2.2.33. информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

2.2.34. сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;

2.2.35. номер расчетного счета;

2.2.36. номер банковской карты.

2.5. Обработка персональных данных муниципальных служащих осуществляется при условии получения согласия указанных лиц в следующих случаях:

2.5.1. при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации о муниципальной службе;

2.5.2. при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

2.6. Согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

2.7. Обработка персональных данных муниципальных служащих осуществляется лицом, ответственным за организацию обработки персональных данных в администрации (далее – Ответственное лицо) и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, удаление, уничтожение персональных данных.

2.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных муниципальных служащих Администрации осуществляется путем:

2.8.1. получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые ответственному лицу Администрации);

2.8.2. копирования оригиналов документов;

2.8.3. внесения сведений в учетные формы (на бумажных и электронных носителях);

2.8.4. формирования персональных данных в ходе кадровой работы;

2.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от муниципальных служащих.

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

2.11. Запрещается получать, обрабатывать и приобщать к личному делу персональные данные муниципального служащего, не предусмотренные пунктом 2.2 настоящего раздела, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.12. При сборе персональных данных ответственное лицо Администрации, осуществляющее сбор (получение) персональных данных непосредственно от муниципальных служащих обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

2.13. Передача и использование персональных данных муниципальных служащих осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

2.14. Условия и порядок обработки персональных данных, установленные настоящим разделом, распространяются на обработку персональных данных руководителей муниципальных учреждений, учредителем которых выступает Администрация.

2.15. Условия и порядок обработки персональных данных, установленные настоящим разделом, распространяются на обработку персональных данных руководителей муниципальных предприятий, учредителем которых выступает Администрация, за исключением подпункта 2.2.34.

3. Условия и порядок обработки персональных данных работников, замещающих должности, не являющиеся должностями муниципальной службы

3.1. Персональные данные работников, замещающих должности, не являющиеся должностями муниципальной службы Администрации (далее - Работники Администрации) обрабатываются в целях обеспечения кадровой работы Администрации, в том числе в целях содействия им в работе, в обучении и должностном росте, обеспечения их личной безопасности и членов их семей, в целях организации информационно-технического обеспечения Администрации, а также в целях обеспечения сохранности принадлежащего им имущества и имущества муниципального органа, учета результатов исполнения ими должностных обязанностей.

3.2. В целях, указанных в пункте 3.1 настоящего раздела, обрабатываются следующие категории персональных данных работников Администрации:

3.2.1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

3.2.2. число, месяц, год рождения;

3.2.3. место рождения;

3.2.4. пол;

3.2.5. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

3.2.6. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

3.2.7. адрес места жительства (адрес регистрации, фактического проживания);

3.2.8. номер контактного телефона или сведения о других способах связи;

3.2.9. реквизиты страхового свидетельства государственного пенсионного страхования;

3.2.10. идентификационный номер налогоплательщика;

3.2.11. реквизиты страхового медицинского полиса обязательного медицинского страхования;

3.2.12. сведения, указанные в свидетельствах государственной регистрации актов гражданского состояния;

3.2.13. семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

3.2.14. сведения о трудовой деятельности;

3.2.15. сведения о воинском учете и реквизиты документов воинского учета;

3.2.16. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

3.2.17. фотография;

3.2.18. сведения о профессиональной переподготовке и (или) повышении квалификации;

3.2.19.информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

3.2.20. номер расчетного счета;

3.2.21. номер банковской карты.

3.3. Согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

3.4. Обработка персональных данных Работников Администрации, осуществляется ответственным лицом Администрации и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, удаление, уничтожение персональных данных.

3.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных Работников Администрации, осуществляется путем:

3.5.1. получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые ответственному лицу Администрации);

3.5.2. копирования оригиналов документов;

3.5.3. внесения сведений в учетные формы (на бумажных и электронных носителях);

3.5.4. формирования персональных данных в ходе кадровой работы;

3.6. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от Работников Администрации.

3.7. В случае возникновения необходимости получения персональных данных Работников Администрации у третьей стороны, следует известить об этом Работников Администрации заранее, получить их письменное согласие и сообщить о целях, предполагаемых источниках и способах получения персональных данных.

3.8. Запрещается получать, обрабатывать и приобщать к личному делу персональные данные Работников Администрации, не предусмотренные пунктом 3.2 настоящего раздела, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

3.9. При сборе персональных данных ответственное лицо Администрации, осуществляющее сбор (получение) персональных данных непосредственно от Работников Администрации, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

3.10. Передача и использование персональных данных Работников Администрации осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

4. Условия и порядок обработки персональных данных граждан, включенных в кадровый резерв Администрации

4.1. Персональные данные граждан, включенных в кадровый резерв, обрабатываются в целях ведения кадровой работы, в том числе при формировании кадрового резерва Администрации.

4.2. В целях формирования кадрового резерва обрабатываются следующие категории персональных данных граждан:

4.2.1. фамилия, имя, отчество;

4.2.2. пол;

4.2.3. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

4.2.4. адрес места жительства (адрес регистрации, фактического проживания);

4.2.5. номер контактного телефона или сведения о других способах связи;

4.2.6. сведения о трудовой деятельности;

4.2.7. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании).

4.3. Согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

4.4. Обработка персональных данных граждан, включенных в кадровый резерв Администрации, осуществляется ответственным лицом и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, удаление, уничтожение персональных данных.

4.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных граждан, включенных в кадровый резерв, осуществляется путем:

4.5.1. получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые ведущим экспертом по кадровым вопросам);

4.5.2. копирования оригиналов документов;

4.5.3. внесения сведений в учетные формы (на бумажных и электронных носителях);

4.5.4. формирования персональных данных в ходе кадровой работы;

4.6. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от граждан, включенных в кадровый резерв Администрации.

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

4.8. Запрещается получать, обрабатывать и приобщать к личному делу персональные данные граждан, включенных в кадровый резерв, не предусмотренные пунктом 4.2 настоящего раздела, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

4.9. При сборе персональных данных ответственное лицо Администрации, осуществляющее сбор (получение) персональных данных непосредственно от граждан, включенных в кадровый резерв Администрации, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

4.10. Передача и использование персональных данных граждан, включенных в кадровый резерв Администрации, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

5. Условия и порядок обработки персональных данных родственников муниципальных служащих

5.1. В Администрации обработка персональных данных родственников муниципальных служащих осуществляется в следующих целях:

5.1.1. обеспечения кадровой работы Администрации, в том числе в целях содействия муниципальным служащим в работе, обеспечения их личной безопасности и членов их семей, а также в целях предоставления муниципальным служащим льгот и гарантий, предусмотренных законодательством для лиц, имеющих (усыновивших) детей, лиц с семейными обязанностями, выполнение требований нормативных правовых актов органов государственного статистического учета;

5.1.2. в связи с рассмотрением вопроса о предоставлении основных, дополнительных государственных гарантий и субсидий.

5.2. В целях, указанных в п.п. 5.1. настоящего раздела, обрабатываются следующие категории персональных данных родственников муниципальных служащих Администрации:

5.2.1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

5.2.2. число, месяц, год рождения;

5.2.3. место рождения;

5.2.4. пол;

5.2.5. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

5.2.6. место работы (адрес, наименование и занимаемая должность);

5.2.7. домашний адрес (адрес регистрации и фактического проживания);

5.2.8. сведения о наличии или отсутствии судимости;

5.2.9. номер контактного телефона или сведения о других способах связи;

5.2.10. сведения о проживании за границей и (или) оформлении документов для выезда на постоянное место жительства в другое государство;

5.2.11 сведения, указанные в справке о доходах, расходах, об имуществе и об обязательствах имущественного характера.

5.3. Обработка персональных данных родственников муниципальных служащих Администрации, осуществляется ответственным лицом и включает в себя следующие действия:

сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, удаление, уничтожение персональных данных.

5.4. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных родственников муниципальных служащих Администрации осуществляется путем:

5.4.1. получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые ответственному лицу Администрации);

5.4.2. копирования оригиналов документов;

5.4.3. внесения сведений в учетные формы (на бумажных и электронных носителях);

5.4.4. формирования персональных данных в ходе кадровой работы;

5.5. Запрещается получать, обрабатывать и приобщать к личному делу персональные данные родственников муниципальных служащих Администрации, не предусмотренные пунктом 5.2 настоящего раздела, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

5.6. Передача и использование персональных данных родственников муниципальных служащих Администрации осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

5.7. Условия и порядок обработки персональных данных, установленные настоящим разделом, распространяются на обработку персональных данных родственников руководителей учреждений и предприятий, учредителем которых выступает Администрация.

6. Условия и порядок обработки персональных данных родственников работников, замещающих должности, не являющиеся должностями муниципальной службы Администрации

6.1. В Администрации обработка персональных данных родственников работников Администрации, осуществляется в целях обеспечения кадровой работы Администрации, в том числе в целях предоставления работникам, замещающим должности, не являющиеся должностями муниципальной службы Администрации льгот и гарантий, предусмотренных законодательством для лиц, имеющих (усыновивших) детей, лиц с семейными обязанностями, выполнение требований нормативных правовых актов органов государственного статистического учета.

6.2. В целях, указанных в п.п. 6.1. настоящего раздела, обрабатываются следующие категории персональных данных родственников работников, замещающих должности, не являющиеся должностями муниципальной службы Администрации:

6.2.1. фамилия, имя, отчество;

6.2.2. число, месяц, год рождения;

6.2.3. место рождения;

6.2.4. пол;

6.2.5. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

6.2.6. место работы (адрес, наименование и занимаемая должность);

6.2.7. домашний адрес (адрес регистрации и фактического проживания);

6.2.8. номер контактного телефона или сведения о других способах связи;

6.2.9. сведения, указанные в свидетельствах государственной регистрации актов гражданского состояния.

6.3. Обработка персональных данных родственников работников Администрации с целями, указанными в п 6.1, в частности сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных, осуществляется ответственным лицом Администрации , путем:

6.3.1. получения оригиналов необходимых документов;

6.3.2. предоставления заверенных в установленном порядке копий документов.

6.4. Передача и использование персональных данных родственников работников Администрации, осуществляется лишь в случаях и в порядке, предусмотренных законодательством Российской Федерации.

6.5. Обработка персональных данных родственников работников Администрации, осуществляется ответственным лицом Администрации и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, удаление, уничтожение персональных данных.

6.6. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных родственников работников Администрации, осуществляется путем:

6.6.1. получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые ведущему эксперту по кадровым вопросам);

6.6.2. копирования оригиналов документов;

6.6.3. внесения сведений в учетные формы (на бумажных и электронных носителях);

6.6.4. формирования персональных данных в ходе кадровой работы;

6.7. Запрещается получать, обрабатывать и приобщать к личному делу персональные данные родственников работников Администрации, не предусмотренные пунктом 6.2 настоящего раздела, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

6.8. Передача и использование персональных данных родственников работников Администрации осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

7. Условия и порядок обработки персональных данных родственников граждан, претендующих на замещение вакантной должности муниципальной службы

7.1. Персональные данные родственников граждан, претендующих на замещение вакантной должности муниципальной службы, обрабатываются в целях обеспечения кадровой работы Администрации, в том числе в целях содействия им в работе, обеспечения их личной безопасности и членов их семей, а также в целях предоставления Работникам льгот и гарантий, предусмотренных законодательством для лиц, имеющих (усыновивших) детей, лиц с семейными обязанностями, выполнение требований нормативных правовых актов органов государственного статистического учета.

7.2. В целях, указанных в пункте 7.1 настоящего раздела, обрабатываются следующие категории персональных данных родственников соискателей на замещение вакантной должности и лиц, включенных в кадровый резерв:

7.2.1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

7.2.2. число, месяц, год рождения;

7.2.3. место рождения;

7.2.4. пол;

7.2.5. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

7.2.6. место работы (адрес, наименование и занимаемая должность);

7.2.7. домашний адрес (адрес регистрации и фактического проживания);

7.2.8. сведения о наличии или отсутствии судимости;

7.2.9. номер контактного телефона или сведения о других способах связи;

7.2.10. сведения о родственниках, проживающих за границей и (или) оформивших документы для выезда на постоянное место жительства в другое государство;

7.2.11. сведения, указанные в справке о доходах, расходах, об имуществе и об обязательствах имущественного характера.

7.3. Обработка персональных данных родственников граждан, претендующих на замещение вакантной должности муниципальной службы, осуществляется ответственным лицом Администрации и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, блокирование, удаление, уничтожение персональных данных.

7.4. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных родственников соискателей на замещение вакантной должности и лиц, включенных в кадровый резерв, осуществляется путем:

7.4.1.получения оригиналов необходимых документов;

7.4.2. копирования оригиналов документов;

7.4.3. внесения сведений в учетные формы (на бумажных и электронных носителях);

7.4.5. формирования персональных данных в ходе кадровой работы.

7.5. Запрещается получать, обрабатывать и приобщать к личному делу персональные данные родственников граждан, претендующих на замещение вакантной должности муниципальной службы, не предусмотренные пунктом 7.2 настоящего раздела, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

7.6. Передача и использование персональных данных родственников соискателей на замещение вакантной должности и лиц, включенных в кадровый резерв, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

8. Условия и порядок обработки персональных данных физических лиц в связи с предоставлением муниципальных услуг и исполнением муниципальных функций, выполнением муниципальных полномочий, возложенных на Администрацию

8.1. В Администрации обработка персональных данных физических лиц осуществляется в целях предоставления муниципальных услуг и исполнения муниципальных функций, выполнением муниципальных полномочий, возложенных на Администрацию нормативными правовыми актами;

8.2. 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.

В соответствии с законодательством Российской Федерации в Администрации подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан и лиц без гражданства.

8.3. В рамках рассмотрения обращений граждан подлежат обработке следующие персональные данные заявителей:

8.3.1. фамилия, имя, отчество (последнее при наличии);

8.3.2. почтовый адрес;

8.3.3. адрес электронной почты;

8.3.4. указанный в обращении контактный телефон;

8.3.5. пол;

8.3.6. персональные данные, указанные заявителем в обращении (жалобе), а также ставшие известными в ходе личного приема или в процессе рассмотрения поступившего обращения.

8.4. При оказании муниципальных услуг осуществляется обработка персональных данных заявителей, указанных в предоставляемых документах, согласно административным регламентам.

8.5. Обработка персональных данных, необходимых в связи с предоставлением муниципальных услуг и исполнением муниципальных функций, выполнением полномочий, возложенных на Администрацию, осуществляется структурными подразделениями Администрации, предоставляющими соответствующие муниципальные услуги и (или) исполняющими муниципальные функции, выполняющие муниципальные полномочия, возложенные на Администрацию, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, удаление, уничтожение персональных данных.

8.6. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, обратившихся в Администрацию для получения муниципальной услуги или в целях исполнения муниципальной функции, выполнения муниципальных полномочий, возложенных на Администрацию НПА осуществляется путем:

8.6.1. получения оригиналов необходимых документов (заявление);

8.6.2. заверения копий документов;

8.6.3. внесения сведений в учетные формы (на бумажных и электронных носителях).

8.7. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (заявителей).

8.8. При предоставлении муниципальной услуги или исполнении муниципальной функции, выполнении муниципальных полномочий, возложенных на Администрацию, Администрацией запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

8.9. При сборе персональных данных уполномоченное должностное лицо структурного подразделения Администрации, осуществляющее получение персональных данных непосредственно от субъектов персональных данных, обратившихся за предоставлением муниципальной услуги или в связи с исполнением муниципальной функции, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

8.10 Передача и использование персональных данных заявителей (субъектов персональных данных) Администрацией осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами, муниципальными нормативными правовыми актами.

9. Условия и порядок обработки персональных данных представителей юридических лиц, обратившихся в Администрацию

9.1. В Администрации обработка персональных данных представителей юридических лиц и муниципальных учреждений, обратившихся в Администрацию, осуществляется в целях реализации закрепленных за Администрацией полномочий.

9.2. Для реализации поставленных в пункте 9.1 целей необходимы следующие персональные данные:

9.2.1. фамилия, имя, отчество (последнее при наличии);

9.2.2. место работы;

9.2.3. пол;

9.2.4. сведения о документе, удостоверяющем личность;

9.2.5. занимаемая должность;

9.2.6. адрес регистрации (почтовый адрес, адрес места жительства);

9.2.7. адрес электронной почты;

9.2.8. идентификационный номер налогоплательщика;

9.2.9. номер телефона;

9.2.10. иные персональные данные представителей юридических лиц, обратившихся в Администрацию, ставшие известные сотрудникам Администрации в ходе выполнения своих должностных обязанностей.

9.3. Обработка персональных данных, необходимых в связи с предоставлением муниципальных услуг и исполнением муниципальных функций, указанных в пункте 9.1 настоящего Положения, осуществляется без согласия субъектов персональных данных в соответствии с пунктом 4 части 1 статьи 6 Федерального закона от 25.07.2006 г. № 152-ФЗ «О персональных данных».

9.4. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, обратившихся в Администрацию для получения муниципальной услуги или в целях исполнения муниципальной функции, выполнения муниципальных полномочий, возложенных на Администрацию НПА, осуществляется путем:

9.4.1. получения оригиналов необходимых документов (заявление);

9.4.2. заверения копий документов;

9.4.3. внесения сведений в учетные формы (на бумажных и электронных носителях);

9.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (заявителей).

9.6. При предоставлении муниципальной услуги или исполнении муниципальной функции, выполнении муниципальных полномочий, возложенных на Администрацию НПА,

Администрацией запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

9.7. При сборе персональных данных уполномоченное должностное лицо структурного подразделения Администрации, осуществляющее получение персональных данных непосредственно от субъектов персональных данных, обратившихся за предоставлением муниципальной услуги или в связи с исполнением муниципальной функции, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

9.8. Передача и использование персональных данных представителей юридических лиц и муниципальных учреждений (субъектов персональных данных) Администрацией осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами, муниципальными нормативными правовыми актами.

10. Условия и порядок обработки персональных данных физических лиц, которые получены в ходе контрольной деятельности Администрации

10.1. В Администрации обработка персональных данных физических лиц осуществляется в целях выполнения возложенных на Администрацию муниципальных функций по осуществлению муниципального контроля.

10.2. Для реализации поставленных в пункте 10.1 целей необходимы следующие персональные данные:

10.2.1. фамилия, имя, отчество (последнее при наличии);

10.2.2. место работы;

10.2.3. пол;

10.2.4. сведения о документе удостоверяющем личность;

10.2.5. занимаемая должность;

10.2.6. адрес регистрации (почтовый адрес, адрес места жительства);

10.2.7. адрес электронной почты;

10.2.8. идентификационный номер налогоплательщика;

10.2.9. номер телефона;

10.2.10. иные персональные данные физических лиц, ставшие известные сотрудникам Администрации полученные в ходе выполнения контрольной деятельности Администрации.

10.3. Сбор, запись, передача, систематизация, накопление и уточнение (обновление, изменение) персональных данных физических лиц, чьи персональные данные получены в ходе контрольной деятельности, осуществляется путем:

10.3.1. получения оригиналов необходимых документов (заявление);

10.3.2. заверения копий документов;

10.3.3. внесения сведений в учетные формы (на бумажных и электронных носителях);

10.4. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (заявителей).

10.5. При осуществлении муниципального контроля Администрации запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

10.6. При сборе персональных данных уполномоченное должностное лицо структурного подразделения Администрации, осуществляющее получение персональных данных непосредственно от лиц, чьи персональные данные получены в ходе контрольной деятельности, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

10.7. Передача и использование персональных данных заявителей (субъектов персональных данных) Администрацией осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

11. Условия и порядок обработки персональных данных физических лиц, в отношении которых составляются протоколы об административных правонарушениях и рассматриваются дела об административных правонарушениях

11.1. В Администрации обработка персональных данных физических лиц осуществляется в целях составления протоколов об административных правонарушениях, рассмотрения дел об административных правонарушениях и исполнения требований Кодекса Российской Федерации об административных правонарушениях.

11.2. Для реализации поставленных в пункте 11.1 целей необходимы следующие персональные данные:

11.2.1. фамилия, имя, отчество (последнее при наличии);

11.2.2. число, месяц и год рождения;

11.2.3. место рождения;

11.2.4. вид, серия, номер документа, удостоверяющего личность;

11.2.5. адрес регистрации и места жительства;

11.2.6. идентификационный номер налогоплательщика;

11.2.7. почтовый адрес;

11.2.8 должность;

11.2.9. адрес электронной почты;

11.2.10. номер телефона;

11.2.11. иные сведения, полученные при рассмотрении дела об административном правонарушении.

11.3. Сбор, запись, передача, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных.

11.4. При исполнении муниципальной функции Администрацией запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

11.5. При сборе персональных данных уполномоченное должностное лицо структурного подразделения Администрации, осуществляющее получение персональных данных непосредственно от субъектов персональных данных в связи с исполнением муниципальной функции обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

11.6. Передача и использование персональных данных физических лиц, в отношении которых рассматриваются дела об административных правонарушениях (субъектов персональных данных) Администрацией осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами, законами субъектов РФ, муниципальными нормативными правовыми актами.

12. Условия и порядок обработки персональных данных уволенных сотрудников Администрации

12.1. Персональные данные уволенных сотрудников обрабатываются в целях обеспечения кадровой работы Администрации, в том числе в целях содействия им в трудоустройстве, обеспечения их личной безопасности и членов их семей, а также в целях обеспечения сохранности принадлежащего им имущества, предоставления информации по запросам государственных, муниципальных органов, выполнения требований Федерального закона от 22.10.2004г. № 125-ФЗ «Об архивном деле в Российской Федерации», Федерального закона от 02.03.2007 г. № 25-ФЗ «О муниципальной службе Российской Федерации», Трудового Кодекса Российской Федерации.

12.2. В целях, указанных в пункте 12.1 настоящего раздела, обрабатываются следующие категории персональных данных уволенных сотрудников Администрации:

12.2.1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

12.2.2. число, месяц, год рождения;

12.2.3. место рождения;

12.2.4. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

12.2.6. пол;

12.2.6. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

12.2.7. адрес места жительства (адрес регистрации, фактического проживания);

12.2.8. номер контактного телефона или сведения о других способах связи;

12.2.9.реквизиты страхового свидетельства государственного пенсионного страхования;

12.2.10. идентификационный номер налогоплательщика;

12.2.11. реквизиты страхового медицинского полиса обязательного медицинского страхования;

12.2.12. сведения, указанные в свидетельствах о государственной регистрации актов гражданского состояния;

12.2.13. серия, номер заграничного паспорта, наименование органа, выдавшего его, дата выдачи;

12.2.14. семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

12.2.15. сведения о трудовой деятельности;

12.2.16. сведения о воинском учете и реквизиты документов воинского учета;

12.2.17. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

12.2.18. сведения об ученой степени;

12.2.19. информация о владении иностранными языками, степень владения;

12.2.20. медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению;

12.2.21.фотография;

12.2.22. сведения о прохождении государственной гражданской службы, в том числе: дата, основания поступления на государственную гражданскую службу и назначения на должность государственной гражданской службы, дата, основания назначения, перевода, перемещения на иную должность государственной гражданской службы, наименование замещаемых должностей государственной гражданской службы с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности государственной гражданской службы, а также сведения о прежнем месте работы (сведения о прохождении муниципальной службы);

12.2.23. информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту;

12.2.24. сведения о беременности;

12.2.25. сведения об инвалидности;

12.2.26. сведения о пребывании за границей;

12.2.27. информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы);

12.2.28. сведения о родственниках, проживающих за границей и (или) оформивших документы для выезда на постоянное место жительства в другое государство;

12.2.29. сведения о наличии или отсутствии судимости;

12.2.30. информация об оформленных допусках к государственной тайне;

12.2.31. государственные награды, иные награды и знаки отличия;

12.2.32.сведения о профессиональной переподготовке и (или) повышении квалификации;

12.2.33. информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

12.2.34. сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;

12.2.35. номер расчетного счета;

12.2.36. номер банковской карты.

12.3. Обработка персональных данных уволенных сотрудников Администрации осуществляется при условии получения согласия указанных лиц в следующих случаях:

12.3.1. при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации о муниципальной службе;

12.3.2. при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

12.4. Обработка персональных данных уволенных сотрудников Администрации осуществляется ответственным лицом Администрации и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, удаление, уничтожение персональных данных.

12.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных уволенных сотрудников Администрации, осуществляется путем:

12.5.1. получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые ответственному лицу Администрации);

12.5.2. копирования оригиналов документов;

12.5.3.внесения сведений в учетные формы (на бумажных и электронных носителях);

12.5.4. формирования персональных данных в ходе кадровой работы.

12.6. Запрещается получать, обрабатывать и приобщать к личному делу персональные данные уволенных сотрудников Администрации, не предусмотренные пунктом 12.2 настоящего раздела, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

12.7. Передача и использование персональных данных уволенных сотрудников Администрации осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

13. Условия и порядок обработки персональных данных граждан, претендующих на замещение вакантных должностей муниципальной службы

13.1. Персональные данные граждан, претендующих на замещение должностей муниципальной службы в Администрации, обрабатываются в целях обеспечения кадровой работы Администрации.

13.2. В целях, указанных в пункте 13.1 настоящего раздела, обрабатываются следующие категории персональных данных граждан, претендующих на замещение муниципальной службы Администрации:

13.2.1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

13.2.2. число, месяц, год рождения;

13.2.3. место рождения;

13.2.4. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

13.2.5. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

13.2.6. адрес места жительства (адрес регистрации, фактического проживания);

13.2.7. номер контактного телефона или сведения о других способах связи;

13.2.8. реквизиты страхового свидетельства государственного пенсионного страхования;

13.2.9. идентификационный номер налогоплательщика;

13.2.10. реквизиты страхового медицинского полиса обязательного медицинского страхования;

13.2.11. реквизиты свидетельства государственной регистрации актов гражданского состояния;

13.2.12. семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

13.2.13. сведения о трудовой деятельности;

13.2.14. сведения о воинском учете и реквизиты документов воинского учета;

13.2.15. сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

13.2.16. сведения об ученой степени;

13.2.17. информация о владении иностранными языками, степень владения;

13.2.18. медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению;

13.2.19. фотография;

13.2.20. сведения о прохождении государственной гражданской службы, в том числе: дата, основания поступления на государственную гражданскую службу и назначения на должность государственной гражданской службы, дата, основания назначения, перевода, перемещения на иную должность государственной гражданской службы, наименование замещаемых должностей государственной гражданской службы с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности государственной гражданской службы, а также сведения о прежнем месте работы (сведения о прохождении муниципальной службы);

13.2.21. информация, содержащаяся в служебном (муниципальном) контракте, дополнительных соглашениях к служебному (муниципальному) контракту;

13.2.22. сведения о пребывании за границей;

13.2.23. информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы);

13.2.24. сведения о наличии или отсутствии судимости;

13.2.25. информация об оформленных допусках к государственной тайне;

13.2.26. государственные награды, иные награды и знаки отличия;

13.2.27. сведения о профессиональной переподготовке и (или) повышении квалификации;

13.2.28. информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

13.2.29.сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;

13.2.30. пол.

13.3. Согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

13.4. Обработка персональных данных граждан, претендующих на замещение должностей муниципальной службы в Администрации, осуществляется ответственным лицом Администрации и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, удаление, уничтожение персональных данных.

13.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных граждан, претендующих на замещение должностей муниципальной службы в Администрации, осуществляется путем:

13.5.1. получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые ответственному лицу Администрации);

13.5.2. копирования оригиналов документов;

13.5.3. внесения сведений в учетные формы (на бумажных и электронных носителях);

13.5.4. формирования персональных данных в ходе кадровой работы.

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

13.7. В случае возникновения необходимости получения персональных данных граждан, претендующих на замещение должностей муниципальной службы в Администрации у третьей стороны следует известить об этом гражданина заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных.

13.8. Запрещается получать, обрабатывать и приобщать к личному делу персональные данные граждан, претендующих на замещение должностей муниципальной службы в Администрации, не предусмотренные пунктом 13.2 настоящего раздела, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

13.9. При сборе персональных данных ответственное лицо Администрации, осуществляющее сбор (получение) персональных данных непосредственно от граждан, претендующих на замещение должностей муниципальной службы Администрации, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

13.10. Передача и использование персональных данных граждан, претендующих на замещение должностей муниципальной службы в Администрации, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

14. Порядок хранения и использования персональных данных

14.1. Хранение персональных данных работников осуществляется на бумажных носителях, а при необходимости и на электронных носителях.

14.2. Доступ к персональным данным, хранящимся на электронных носителях, а также к программному обеспечению регламентирован и осуществляется при введении пароля, использования электронной подписи иных средств защиты от несанкционированного доступа.

14.3. Документы (на бумажных носителях), содержащие ПДн, хранятся в шкафах работников, ответственных за ведение и хранение таких документов.

14.4. Помещения, в которых хранятся персональные данные работников, оборудуются средствами физической защиты (двери, замки, сигнализация).

14.5. Обработка персональных данных в Администрации осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, исполнения работодателем договорных обязательств.

14.6. Допуск к персональным данным разрешен должностным лицам, включенным в Перечень должностей, которым персональные данные необходимы для выполнения конкретных трудовых функций.

14.7. К персональным данным, обрабатываемым в Администрации, могут допускаться работники контрольно-ревизионных органов при наличии документов, являющихся основанием к работе с персональными данными.

14.8. Работники, обрабатывающие персональные данные с использованием и без использования средств автоматизации, обязаны обеспечивать их безопасность от несанкционированного доступа к ним и копирования.

14.9. Работники, допущенные к обработке персональных данных, обязаны:

а) осуществлять передачу персональных данных работников в пределах организации в соответствии с Перечнем должностей;

б) предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

в) разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

г) передавать персональные данные работника представителям работников в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

14.10. Работникам, допущенным к обработке персональных данных, запрещается:

а) сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных законодательством Российской Федерации;

б) сообщать персональные данные работника в коммерческих целях без его письменного согласия;

в) запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

14.11. Защита персональных данных работников от их неправомерного использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном законодательством Российской Федерации.

15. Уничтожение персональных данных

15.1. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном законодательством Российской Федерации.

15.2. Персональные данные работников подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении таких целей.

15.3. Уничтожение документов, содержащих персональные данные, производится комиссионно. Комиссия назначается распоряжением администрации муниципального округа. По результатам работы комиссии оформляются акты об уничтожении.

16. Права субъектов персональных данных

16.1.Субъекты персональных данных имеют право на:

а) полную информацию о своих персональных данных и обработке этих данных;

б) свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законодательством;

в) определение своих представителей для защиты своих персональных данных;

г) требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства Российской Федерации;

д) требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

е) обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите своих персональных данных.

17. Ответственность работников при обработке персональных данных

17.1. Работники Администрации при приеме на работу проходят инструктаж относительно принятых в администрации муниципального округа мер по защите персональных данных и порядке их обработки, после чего дают согласие на обработку своих персональных данных и обязательство о неразглашении персональных данных и иной конфиденциальной информации.

17.2. Разглашение персональных данных, то есть передача посторонним лицам, не имеющим к ним доступа; публичное раскрытие; утрата документов и иных носителей,

содержащих персональные данные работника; иные нарушения обязанностей по их защите, обработке и хранению влекут наложение дисциплинарного взыскания - выговора, увольнения.

В случае причинения организации ущерба, связанного с нарушением правил обработки и защиты персональных данных работник несёт материальную ответственность в соответствии с п. 7 ч. 1 ст. 243 Трудового кодекса РФ.

В случае незаконного собирания или распространения работником сведений о частной жизни лица, составляющих его личную или семейную тайну, без согласия субъекта ПДн либо распространения этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации он несет уголовную ответственность.

17.3. Настоящие Правила обязательны для всех сотрудников администрации муниципального округа.

17. 4. В соответствии с требованиями п. 8 ст. 86 Трудового кодекса Российской Федерации, работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

18. Меры, принимаемые в Администрации, для защиты персональных данных

18.1 Мерами, принимаемыми в Администрации для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, являются:

а) назначение ответственных за организацию обработки и обработку персональных данных, за обеспечение безопасности персональных данных при работе в информационных системах;

б) актуализация нормативной базы;

в) ознакомление сотрудников с нормативными документами под роспись;

г) определение Перечней категорий персональных данных, обрабатываемых в Администрации;

д) определение Перечня должностей, имеющих доступ к персональным данным;

е) определение мест хранения материальных носителей персональных данных в администрации муниципального округа

ж) утверждение порядка доступа работников администрации муниципального округа в помещения, где обрабатываются персональные данных;

з) реализация требований по парольной и иной защите доступа к информационным ресурсам;

и) определение порядка размещения мониторов на рабочих местах пользователей, исключающий просмотр визуальной информации посторонними лицами;

к) обеспечение защиты от воздействия вредоносных программ и программно-математических воздействий (антивирусная защита, администрирование);

л) передача обрабатываемых персональных данных по общедоступной телекоммуникационной сети (Интернет) с использованием сертифицированных программных средств защиты информации;

м) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

н) учет машинных носителей персональных данных;

о) обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

п) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

р) организация контроля выполнения условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

Приложение № 2 к постановлению администрации Солигаличского муниципального округа Костромской

области от 27 марта 2024 года № 367

ТИПОВАЯ ФОРМА
согласия на обработку персональных данных

г.Солигалич "___" _____ 20 ___г.

Я, _____
(наименование документа, удостоверяющего личность,
_____
серия и номер, дата выдачи и наименование органа, выдавшего документ)

зарегистрированный(ая) по адресу: _____
_____

в соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных» принимаю решение о предоставлении своих персональных данных и свободно, своей волей и в своем интересе даю согласие администрации Солигаличского муниципального округа Костромской области, расположенной по адресу: 157170, Костромская область, город Солигалич, ул. Коммунистическая, д.1, на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) следующих персональных данных:

фамилия, имя, отчество, дата и место рождения, гражданство;

прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);

владение иностранными языками и языками народов Российской Федерации;

образование (когда и какие образовательные организации закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);

послевузовское профессиональное образование (наименование образовательной или научной организации, год окончания), ученая степень, ученое выполняемая работа с начала трудовой деятельности;

классный чин федеральной государственной гражданской службы, гражданской службы субъекта Российской Федерации, муниципальной службы, дипломатический ранг, воинское, специальное звание, классный чин правоохранительной службы, юстиции (кем и когда присвоены);

государственные награды, иные награды и знаки отличия (кем награжден и когда);

степень родства, фамилии, имена, отчества, даты и места рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);

места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);

фамилии, имена, отчества, даты рождения, места рождения, места работы и домашние адреса бывших мужей (жен);

пребывание за границей (когда, где, с какой целью);

близкие родственники (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывшие, постоянно проживающие за границей и (или) оформляющие документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей);

адрес и дата регистрации по месту жительства, адрес фактического проживания;

паспорт (серия, номер, кем и когда выдан);

паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан);

отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);

номер страхового свидетельства обязательного пенсионного страхования;

реквизиты полиса обязательного медицинского страхования;

наличие (отсутствие) судимости;

допуск к государственной тайне, оформленный за период работы, службы, учебы (форма, номер, дата);

сведения о наличии (отсутствии) заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению, а также результаты обязательных периодических медицинских осмотров (обследований);

сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах об имуществе и обязательствах имущественного характера своих супруги (супруга) и несовершеннолетних детей;

сведения о профессиональных достижениях и заслугах;

фотография;

сведения о социальных льготах, на которые работник имеет право в соответствии с действующим законодательством Российской Федерации;

реквизиты расчетного счета банковской карты;

сведения о заработке от других страхователей для расчета пособий;

иные персональные данные, необходимые для достижения целей их обработки;

Вышеуказанные персональные данные предоставляю для обработки в целях осуществления и выполнения администрацией Солигаличского муниципального округа Костромской области функций, полномочий и обязанностей в сфере трудовых и служебных отношений в соответствии с действующим законодательством Российской Федерации.

Разрешаю обмен (прием, передачу, обработку) моих персональных данных между администрацией Солигаличского муниципального округа Костромской области и третьими лицами в целях соблюдения моих законных прав и интересов.

Я ознакомлен(а) с тем, что:

согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока осуществления и выполнения администрацией Солигаличского муниципального округа Костромской области функций, полномочий и обязанностей в сфере трудовых и служебных отношений в соответствии с действующим законодательством Российской Федерации;

персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться администрацией Солигаличского муниципального округа Костромской области только в целях осуществления и выполнения функций, полномочий и обязанностей в сфере трудовых и служебных отношений в соответствии с действующим законодательством Российской Федерации;

согласие на обработку персональных данных может быть отозвано мной на основании письменного заявления в произвольной форме;

в случае отзыва согласия на обработку персональных данных администрация Солигаличского муниципального округа Костромской области вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 года N 152-ФЗ «О персональных данных»;

после осуществления и выполнения администрацией Солигаличского муниципального округа Костромской области функций, полномочий и обязанностей в сфере трудовых и служебных отношений в соответствии с действующим законодательством Российской Федерации персональные данные хранятся в администрации Солигаличского муниципального округа в течение срока хранения документов, предусмотренных законодательством Российской Федерации.

Начало обработки персональных данных _____

(число, месяц, год)

_____

(подпись, расшифровка подписи)

Приложение № 3 к постановлению администрации Солигаличского

муниципального округа Костромской области от 27 марта 2024 года № 367

Главе Солигаличского муниципального округа Костромской области

_____

от _____

(Ф.И.О.)

_____

(должность)

_____

(дата рождения)

проживающего по адресу: _____

_____

паспорт:_____

выдан: _____

_____

Форма согласия на получение персональных данных у третьей стороны

Я, _____ в соответствии со ст.86 ТК РФ согласен / не согласен (нужное подчеркнуть) на получение моих персональных данных у третьей стороны, а именно:

_____

_____

(указать Ф.И.О. физического лица или наименование организации, у которых получается информация)

О целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение предупрежден.

"____" _____20___г.

_____ _____

(подпись) (Ф.И.О. работника)

Приложение № 4 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Главе Солигаличского муниципального округа Костромской области

_____

от _____

(Ф.И.О.)

_____

(должность)

_____

(дата рождения)

проживающего по адресу: _____

_____

паспорт:_____

выдан: _____

_____

ЗАЯВЛЕНИЕ

об отзыве согласия на обработку персональных данных

На основании пункта 2 статьи 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», отзываю ранее данное мной согласие на обработку персональных данных.

В случае, если согласие на обработку персональных данных давалось мной неоднократно, настоящим я отзываю все ранее данные мной согласия на обработку персональных данных.

В соответствии с пунктом 5 статьи 21 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», в случае отзыва субъектом персональных данных согласия на их обработку, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва.

Я уведомлен, что в случае отзыва согласия на обработку персональных данных, администрация Солигаличского муниципального округа Костромской области вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Уведомление о прекращении обработки и уничтожении моих персональных данных прошу предоставить в письменной форме.

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Приложение № 5 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

ТИПОВАЯ ФОРМА
разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Мне, _____,

разъяснены юридические последствия отказа предоставить администрации Солигаличского муниципального округа Костромской области свои персональные данные.

Я предупрежден(а), что в случае отказа предоставления своих персональных данных администрация Солигаличского муниципального округа Костромской области не сможет осуществлять обработку персональных данных.

Мне известно, что администрация Солигаличского муниципального округа Костромской области для осуществления и выполнения функций, полномочий и обязанностей в сфере трудовых и служебных отношений в соответствии с действующим законодательством Российской Федерации вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Приложение № 6 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
муниципального служащего администрации Солигаличского муниципального округа Костромской области, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку

персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я, _____

(фамилия, имя, отчество, должность)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора (контракта), освобождения меня от замещаемой должности и увольнения с муниципальной службы.

В соответствии со статьей 7 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Мне разъяснена ответственность, предусмотренная Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и другими федеральными законами.

«____» _____ 20 _____ г. _____ _____

(дата) (подпись) (расшифровка подписи)

Приложение № 7 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Форма листа ознакомления муниципального служащего (работника) администрации Солигаличского муниципального округа Костромской области, непосредственно осуществляющего обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных)

Я,_____

(фамилия, имя, отчество)

_____

(должность)

ознакомлен(а) с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных.

Мною изучены положения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федерального закона от 2 марта 2007 года № 25-ФЗ «О муниципальной службе в Российской Федерации», Трудового кодекса Российской Федерации, Постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановления Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», муниципальными нормативными правовыми актами, определяющими политику в отношении обработки персональных данных в администрации Солигаличского муниципального округа Костромской области, иными документами, определяющими политику в отношении обработки персональных данных.

Я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Ответственность и права, предусмотренные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснены.

«____» _____ 20 _____ г. _____ _____
(дата) (подпись) (расшифровка подписи)

Приложение № 8 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации Солигаличского муниципального округа Костромской области

1. Настоящими Правилами рассмотрения запросов субъектов персональных данных или их представителей в администрации Солигаличского муниципального округа Костромской области (далее - Правила) определяется порядок учета (регистрации) и рассмотрения запросов субъектов персональных данных или их представителей (далее - запросы).

2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), Федеральным законом от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральным законом от 2 марта 2007 года № 25-ФЗ «О муниципальной службе в Российской Федерации», Трудовым кодексом Российской Федерации, постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации» и другими нормативными правовыми актами.

3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

а) подтверждение факта обработки персональных данных в администрации муниципального округа;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые в администрации муниципального округа способы обработки персональных данных;

г) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

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

е) порядок осуществления субъектом персональных данных прав, предусмотренных настоящими Правилами;

ж) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

з) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению главы Солигаличского муниципального округа Костромской области, если обработка поручена или будет поручена такому лицу;

и) иные сведения, предусмотренные федеральными законами.

4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона N 152-ФЗ.

5. Субъект персональных данных вправе требовать от уполномоченных должностных лиц администрации муниципального округа уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6. Сведения, указанные в пункте 3 настоящих Правил, предоставляются субъекту персональных данных или его представителю при направлении запроса субъекта персональных данных или его представителя в администрации муниципального округа.

7. Сведения, указанные в пункте 3 настоящих Правил, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться

персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

8. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с администрацией муниципального округа (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных администрацией муниципального округа, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

9. Рассмотрение запросов является служебной обязанностью уполномоченного должностного лица администрации муниципального округа, в чьи обязанности входит обработка персональных данных.

10. Уполномоченные должностные лица администрации муниципального округа обеспечивают:

а) объективное, всестороннее и своевременное рассмотрения запроса;

б) принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

в) направление письменных ответов по существу запроса.

11. Ведение делопроизводства по запросам субъектов персональных данных или их представителей осуществляется отделом организационно-контрольного обеспечения и делопроизводства администрации муниципального округа.

12. Все поступившие запросы регистрируются в день их поступления. На запросе проставляется штамп, в котором указывается входящий номер и дата регистрации и передается в орган администрации муниципального округа, осуществляющий обработку персональных данных субъекта.

13. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской.

14. В случае если сведения, указанные в пункте 3 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в администрацию муниципального округа или направить повторный запрос в целях получения сведений, указанных в пункте 3 настоящих Правил, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом.

15. Субъект персональных данных вправе обратиться повторно в администрацию муниципального округа или направить повторный запрос в целях получения сведений, указанных в пункте 3 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

16. Администрация муниципального округа вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона N 152-ФЗ, с указанием оснований для такого отказа.

17. Прошедшие регистрацию запросы в тот же день направляются главе администрации муниципального округа либо лицу, исполняющему его обязанности, который дает по каждому из них письменные указания.

18. Должностное лицо, уполномоченное рассматривать запрос, обязано:

а) разобраться в существе запроса, в случае необходимости истребовать дополнительные материалы или осуществить проверку фактов, изложенных в запросах, принять другие меры

для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;

б) принимать законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;

в) сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

19. В ответе администрации муниципального округа сообщается информация о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляется возможность ознакомления с этими персональными данными при личном обращении субъекта персональных данных или его представителя.

20. Отказ в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных, готовит уполномоченное должностное лицо администрации муниципального округа в письменной форме. Отказ должен содержать ссылку на положение части 8 статьи 14 Федерального закона N 152-ФЗ или иного федерального закона, являющуюся основанием для такого отказа. Отказ должен быть подготовлен в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

21. Возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных, предоставляется субъекту персональных данных или его представителю бесплатно.

22. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица администрации муниципального округа обязаны внести в них необходимые изменения.

23. Уполномоченные должностные лица администрации муниципального округа обязаны уведомить субъект персональных данных или его представителя о внесенных изменениях и принять меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

24. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные должностные лица администрации муниципального округа обязаны уничтожить такие персональные данные.

25. В случае поступления сведений о неправомерной обработке персональных данных при обращении либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных, уполномоченные должностные лица администрации муниципального округа обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

26. В случае выявления неправомерной обработки персональных данных уполномоченные должностные лица администрации муниципального округа в срок, не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченные должностные лица в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных администрация муниципального округа обязана уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также уведомляется указанный орган.

27. В случае выявления неточных персональных данных при обращении либо по запросу субъекта персональных данных или его представителя или по запросу уполномоченного органа по защите прав субъектов персональных данных, уполномоченные должностные лица администрации муниципального округа обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

28. В случае подтверждения факта неточности персональных данных уполномоченные должностные лица на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, обязаны уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

29. При необходимости для проверки фактов, изложенных в запросах субъектов персональных данных или их представителей, в администрации муниципального округа организуются служебные проверки в соответствии с муниципальными правовыми актами.

30. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения должностным лицом администрации муниципального округа действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается в правоохранительные органы. Результаты служебной проверки докладываются главе администрации муниципального округа.

31. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

32. Ответы на запросы печатаются на бланке установленной формы и регистрируются в соответствии с правила делопроизводства в администрации муниципального округа.

33. Контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов осуществляется отделом организационно-контрольного обеспечения и делопроизводства администрации муниципального округа.

34. При осуществлении контроля обращается внимание на сроки исполнения поручений по запросам и полноту рассмотрения поставленных вопросов, объективность проверки фактов, изложенных в запросах, законность и обоснованность принятых по ним решений, своевременность их исполнения и направления ответов заявителям.

35. Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц администрации муниципального округа ответственность в соответствии с законодательством Российской Федерации.

Приложение 1 к правилам рассмотрения запросов субъектов персональных данных или их представителей

Форма запроса на предоставление информации, касающейся обработки персональных данных субъекта персональных данных

_____
(наименование или Ф.И.О. оператора)
от _____
(Ф.И.О. субъекта персональных данных)
адрес: _____
телефон: _____, факс _____
электронный адрес: _____

ЗАПРОС

В период с «____» _____ _____ г. по «____» _____ _____ г. обрабатывались следующие персональные данные: _____

_____
_____
(перечень обрабатываемых персональных данных)
с целью _____
(цель обработки персональных данных)
в форме _____
(способы обработки персональных данных)
субъекта персональных данных - _____
_____
(Ф.И.О., паспортные данные, в том числе дата выдачи, выдавший орган)
оператором - _____
_____
(наименование или Ф.И.О. оператора, ИНН, адрес)
Обработка проводилась в рамках _____
_____.
(номер, дата договора либо сведения, иным образом подтверждающие факт обработки персональных данных оператором)
В связи с _____
_____
(обоснование причин)
и на основании частей 3 и 7 статьи 14, статьи 18, части 1 статьи 20 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» прошу предоставить следующую информацию, касающуюся обработки указанных персональных данных:
_____
_____
(существо запроса)
_____,
в следующем порядке _____в срок до «____» _____ _____ года.

Субъект персональных данных _____ _____
(подпись) (ФИО)

Приложение 2 к правилам рассмотрения запросов субъектов персональных данных или их представителей

ЖУРНАЛ
регистрации запросов субъектов персональных данных или их представителей

Начат «____» _____20_____г.
Окончен «____» _____20_____г.

№ п/п	ФИО субъекта	Дата обращения	Содержание запроса	Отметка об исполнении	ФИО исполнителя	Подпись

Приложение № 9 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Солигаличского муниципального округа Костромской области

1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Солигаличского муниципального округа Костромской области (далее - Правила) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации", Постановлением Правительства Российской Федерации от 21 марта 2012 года N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" и другими нормативными правовыми актами.

3. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных".

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным в администрации муниципального округа требованиям организовывается проведение периодических проверок условий обработки персональных данных.

5. Проверки осуществляются должностными лицами, ответственным за организацию обработки персональных данных в администрации муниципального округа, либо комиссией, образуемой распоряжением администрации муниципального округа.

В проведении проверки не может участвовать муниципальный служащий, прямо или косвенно заинтересованный в её результатах.

6. Проверки соответствия обработки персональных данных установленным в администрации муниципального округа требованиям проводятся на основании поступившего в администрации муниципального округа письменного заявления о нарушениях правил обработки персональных данных либо по поручению главы администрации муниципального округа. Проведение проверки организуется в течение трех рабочих дней со дня поступления соответствующего заявления.

7. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

а) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

б) порядок и условия применения средств защиты информации;

в) эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

г) состояние учета машинных носителей персональных данных;

д) соблюдение правил доступа к персональным данным;

е) наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

ж) мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

з) осуществление мероприятий по обеспечению целостности персональных данных.

8. Лица, ответственные за организацию обработки персональных данных в администрации муниципального округа (комиссия) имеет право:

а) запрашивать у муниципальных служащих (работников) администрации муниципального округа информацию, необходимую для реализации полномочий;

б) требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

в) принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

г) вносить главе Солигаличского муниципального округа Костромской области предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

д) вносить главе администрации муниципального округа предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

9. В отношении персональных данных, ставших известными лицу, ответственному за организацию обработки персональных данных в администрации муниципального округа (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

10. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, главе администрации муниципального округа докладывает лицо, ответственное за организацию обработки персональных данных, либо председатель комиссии, в форме письменного заключения.

11. Глава Солигаличского муниципального округа Костромской области, назначивший внеплановую проверку, контролирует своевременность и правильность её проведения.

Приложение № 10 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Правила работы с обезличенными данными в администрации Солигаличского муниципального округа Костромской области в случае обезличивания персональных данных

1. Настоящие Правила работы с обезличенными персональными данными, обрабатываемыми в администрации Солигаличского муниципального округа Костромской области, (далее - Правила) разработаны в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации" и определяют порядок работы с обезличенными персональными данными в администрации Солигаличского муниципального округа Костромской области.

2. В настоящих Правилах используются термины и определения, установленные Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных".

3. Обезличивание персональных данных в администрации муниципального округа проводится с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижение класса информационных систем персональных данных.

4. Способами обезличивания персональных данных при условии их дальнейшей обработки являются:

а) уменьшение перечня обрабатываемых сведений;

б) замена части сведений идентификаторами;

в) обобщение - понижение точности некоторых сведений;

г) понижение точности некоторых сведений (например, "Место жительства" может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

д) деление сведений на части и обработка в разных информационных системах;

е) иные способы.

5. Способом обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

6. Перечень должностей муниципальных служащих администрации Солигаличского муниципального округа Костромской области, ответственных за проведение мероприятий по обезличиванию персональных данных, утверждается распоряжением администрации Солигаличского муниципального округа Костромской области.

7. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

8. Обезличенные персональные данные обрабатываются с использованием и без использования автоматизации.

9. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

а) парольной политики;

б) антивирусной политики;

в) правил работы со съемными носителями (если они используются);

г) правил резервного копирования;

д) правил доступа в помещения, где расположены элементы информационных систем.

10. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

а) правил хранения бумажных носителей;

б) правил доступа к ним и в помещения, где они хранятся.

Приложение № 11 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Перечень персональных данных, обрабатываемых в администрации Солигаличского муниципального округа Костромской области, в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций

1. Перечень персональных данных, обрабатываемых в администрации Солигаличского муниципального округа Костромской области в связи с реализацией служебных или трудовых отношений:

1.1. Фамилия, имя, отчество, дата и место рождения, гражданство.

1.2. Прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения).

1.3. Владение иностранными языками и языками народов Российской Федерации.

1.4. Образование (когда и какие образовательные организации закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому).

1.5. Послевузовское профессиональное образование (наименование образовательной или научной организации, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов).

1.6. Выполняемая работа с начала трудовой деятельности.

1.7. Классный чин федеральной государственной гражданской службы, гражданской службы субъекта Российской Федерации, муниципальной службы, дипломатический ранг,

воинское, специальное звание, классный чин правоохранительной службы, юстиции (кем и когда присвоены).

1.8. Государственные награды, иные награды и знаки отличия (кем награжден и когда).

1.9. Степень родства, фамилии, имена, отчества, даты и места рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены).

1.10. Места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены).

1.11. Фамилии, имена, отчества, даты рождения, места рождения, места работы и домашние адреса бывших мужей (жен).

1.12. Пребывание за границей (когда, где, с какой целью).

1.13. Близкие родственники (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывшие, постоянно проживающие за границей и (или) оформляющие документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей).

1.14. Адрес и дата регистрации по месту жительства, адрес фактического проживания.

1.15. Паспорт (серия, номер, кем и когда выдан).

1.16. Паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан).

1.17. Номер телефона.

1.18. Отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу).

1.19. Идентификационный номер налогоплательщика.

1.20. Номер страхового свидетельства обязательного пенсионного страхования.

1.21. Реквизиты полиса обязательного медицинского страхования.

1.22. Наличие (отсутствие) судимости.

1.23. Допуск к государственной тайне, оформленный за период работы, службы, учебы (форма, номер, дата).

1.24. Сведения о наличии (отсутствии) заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению, а также результаты обязательных периодических медицинских осмотров (обследований).

1.25. Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах об имуществе и обязательствах имущественного характера своих супруги (супруга) и несовершеннолетних детей.

1.26. Сведения о профессиональных достижениях и заслугах.

1.27. Фотография.

1.28. Сведения о социальных льготах, на которые работник имеет право в соответствии с действующим законодательством Российской Федерации.

1.29. Реквизиты расчетного счета, банковской карты.

1.30. Сведения о заработке от других страхователей для расчета пособий.

1.31. Справка о доходах физического лица по форме 2-НДФЛ.

2. Перечень персональных данных, обрабатываемых в администрации Солигаличского муниципального округа Костромской области в связи с оказанием муниципальных услуг и осуществлением муниципальных функций:

2.1. Фамилия, имя, отчество.

2.2. Паспортные данные.

2.3. Дата рождения.

2.4. Адрес места жительства (по паспорту и фактический).

2.5. Контактный телефон.

2.6. Номер страхового свидетельства государственного пенсионного страхования.

2.7. № и серия свидетельства о рождении ребенка.

2.8. № и серия медицинского полиса.

2.9. Сведения о социальных льготах.

2.10. Социальное положение семьи.

2.11. Сведения о составе семьи.

2.12. Сведения о жилищных условиях и жилой площади.
2.13. Сведения об объектах недвижимости.

Приложение № 12 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Перечень должностей в администрации Солигаличского муниципального округа Костромской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, в том числе работу с информационными системами, базами данных, содержащими персональные данные

1. аппарат главы Солигаличского муниципального округа Костромской области:
первый заместитель главы администрации;
заместитель главы администрации;
управляющий делами администрации;
консультант по вопросам осуществления внутреннего финансового контроля;
консультант по вопросам опеки и попечительства
2. финансовое управление администрации:
начальник финансового управления;
заместитель начальника финансового управления – начальник бюджетного отдела;
заместитель начальника финансового управления – начальник отдела по учету и отчетности;
заместитель начальника отдела по учету и отчетности;
заместитель начальника бюджетного отдела;
консультант отдела по учету и отчетности;
консультант бюджетного отдела;
главный специалист отдела по учету и отчетности;
ведущий специалист бюджетного отдела
3. отдел по экономическому развитию:
заведующий отделом;
заместитель заведующего отделом;
главный специалист отдела;
4. отдел по строительству и архитектуре администрации
заведующий отделом;
заместитель заведующего отделом, главный архитектор;
главный специалист отдела.
5. отдел по управлению имуществом и земельными ресурсами администрации:
заведующий отделом;
заместитель заведующего отделом;
главный специалист, эколог отдела;
консультант отдела;
главный специалист;
6. отдел по делам культуры, молодежи и спорта администрации:
заведующий отделом;
главный специалист отдела;
7. отдел образования администрации:
заведующий отделом;
заместитель заведующего отделом;
главный специалист;
8. отдел по делам сельского хозяйства администрации:
заведующий отделом;
главный специалист отдела;

9. юридический отдел администрации:
заведующий юридическим отделом;
заместитель заведующего юридическим отделом;
главный специалист по охране труда юридического отдела;
10. сектор по делам архивов администрации
заведующий сектором по делам архивов;
ведущий специалист сектора по делам архивов;
11. главный специалист, секретарь комиссии по делам несовершеннолетних и защите их прав;
12. отдел по вопросам жилищно-коммунального хозяйства и благоустройства территорий:
заведующий отделом;
заместитель заведующего отделом;
консультант;
главный специалист;
специалист по связям с общественностью.

Приложение № 13 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Перечень должностей муниципальной службы в администрации Солигаличского муниципального округа Костромской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

1. аппарат главы Солигаличского муниципального округа Костромской области:
первый заместитель главы администрации;
заместитель главы администрации;
заместитель главы администрации-заведующий отделом по делах сельского хозяйства;
управляющий делами администрации;
помощник главы Солигаличского муниципального округа по мобилизационной работе, гражданской обороне и чрезвычайным ситуациям;
консультант по вопросам осуществления внутреннего финансового контроля;
главный специалист по вопросам опеки и попечительства.
2. финансовое управление администрации:
начальник финансового управления;
заместитель начальника финансового управления – начальник бюджетного отдела;
заместитель начальника финансового управления – начальник отдела по учету и отчетности;
заместитель начальника отдела по учету и отчетности;
заместитель начальника бюджетного отдела;
консультант отдела по учету и отчетности;
консультант бюджетного отдела;
главный специалист отдела по учету и отчетности;
ведущий специалист бюджетного отдела
3. отдел по экономическому развитию, строительству и архитектуре администрации
заведующий отделом;
заместитель заведующего отделом, главный архитектор;
главный специалист отдела;
ведущий специалист отдела;
4. отдел по управлению имуществом и земельными ресурсами администрации:
заведующий отделом;
заместитель заведующего отделом;
главный специалист, эколог отдела;

ведущий специалист отдела;

5. отдел по делам культуры, молодежи и спорта администрации:

заведующий отделом;

главный специалист отдела;

6. отдел образования администрации:

заведующий отделом;

заместитель заведующего отделом;

главный специалист;

7. отдел по делам сельского хозяйства администрации:

главный специалист отдела;

8. юридический отдел администрации:

заведующий юридическим отделом;

заместитель заведующего юридическим отделом;

главный специалист по охране труда юридического отдела;

9. сектор по делам архивов администрации

заведующий сектором по делам архивов;

ведущий специалист сектора по делам архивов;

10. главный специалист, секретарь комиссии по делам несовершеннолетних и защите их прав.

Приложение № 14 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Должностная инструкция ответственного за организацию обработки персональных данных в администрации Солигаличского муниципального округа Костромской области

1. Общие положения

1.1. Должностное лицо администрации Солигаличского муниципального округа Костромской области, ответственное за организацию обработки персональных данных назначается и освобождается главой Солигаличского муниципального округа Костромской области.

1.2. Должностное лицо, ответственное за организацию обработки персональных данных, должно руководствоваться в своей деятельности Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации", и другими нормативными правовыми актами, муниципальными правовыми актами, настоящей должностной инструкцией.

2. Должностные обязанности

Должностное лицо, ответственное за организацию обработки персональных данных выполняет следующие обязанности:

а) предоставляет субъекту персональных данных по его просьбе информацию;

б) осуществляет внутренний контроль за соблюдением требований законодательства РФ при обработке персональных данных в администрации муниципального округа, в том числе требований к защите персональных данных;

в) доводит до сведения муниципальных служащих положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

г) организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов;

д) разъясняет субъекту персональных данных юридические последствия отказа предоставления его персональных данных.

3. Права

Должностное лицо, ответственное за организацию обработки персональных данных вправе:

а) запрашивать и получать в установленном порядке от субъектов персональных данных или их представителей сведения, содержащие персональные данные;

б) распоряжаться полученными персональными данными в пределах, установленных законодательством;

в) в установленном порядке пользоваться система связи, информационными базами данных и иными носителя информации Администрации.

4. Ответственность

4.1. Должностное лицо, ответственное за организацию обработки персональных данных, в соответствии со своими полномочиями владеющее информацией о субъектах персональных данных, получающее и использующие её, несет ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки, использования, хранения и передачи персональных данных.

4.2. Должностное лицо, виновное в нарушении установленного законом порядка сбора, хранения, использования, распространения или защиты персональных данных, несет дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

С должностной инструкцией ознакомлен:

_____

(подпись, фамилия имя отчество)

"__" _____ 20___года

Приложение № 15 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Порядок доступа в помещения, в которых ведется обработка персональных данных

1. Настоящий Порядок доступа в помещения, в которых ведется обработка персональных данных (далее - Порядок) разработан в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации" и устанавливает единые требования к доступу в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в администрации Солигаличского муниципального округа Костромской области (далее – администрация муниципального округа), и обеспечения соблюдения требований законодательства о персональных данных.

2. Настоящий Порядок обязателен для применения и исполнения всеми работниками администрации муниципального округа.

3. Персональные данные относятся к конфиденциальной информации. Должностные лица администрации муниципального округа, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

4. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установлением правил доступа в помещения, где обрабатываются персональные данные в информационной системе персональных данных и без использования средств автоматизации.

5. Помещения, в которых ведется обработка персональных данных, должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами и оснащены охранной сигнализацией либо охраной.

6. Персональные данные на бумажных носителях должны находиться в недоступном для посторонних лиц месте.

7. Бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) хранятся в металлических шкафах.

8. Помещения, в которых ведется обработка персональных данных, запираются на ключ.

9. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании рабочего времени работники, имеющие право доступа в помещения, обязаны:

- убрать бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) в шкафы;

- отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

- закрыть окна.

10. Перед открытием помещений, в которых ведется обработка персональных данных, работники, имеющие право доступа в помещения, обязаны провести внешний осмотр с целью установления целостности двери и замка;

11. При обнаружении неисправности двери и запирающих устройств работники обязаны:

- не вскрывая помещение, в котором ведется обработка персональных данных, доложить непосредственному руководителю;

- в присутствии не менее двух иных работников, включая непосредственного руководителя, вскрыть помещение и осмотреть его;

- составить акт о выявленных нарушениях и передать его главе администрации для организации служебного расследования.

12. Право самостоятельного входа в помещения, где обрабатываются персональные данные, имеют только работники, непосредственно работающие в данном помещении.

Иные работники имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии работников, непосредственно работающих в данных помещениях.

13. При работе с информацией, содержащей персональные данные, двери помещений должны быть всегда закрыты.

Присутствие иных лиц, не имеющих права доступа к персональным данным, должно быть исключено.

14. Техническое обслуживание компьютерной и организационной техники, сопровождение программных средств, уборка помещения, в котором ведется обработка персональных данных, а также проведение других работ осуществляются в присутствии работника, работающего в данном помещении.

15. В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещение, в котором ведется обработка персональных данных, вскрывается комиссией в составе не менее двух человек.

16. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на руководителей структурных подразделений администрации муниципального округа, обрабатывающих персональные данные.

Приложение № 16 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Положение об экспертной комиссии администрации Солигаличского муниципального округа Костромской области

1. Общие положения

1.1. Экспертная комиссия администрации Солигаличского муниципального округа Костромской области (далее экспертная комиссия, комиссия) образована в целях организации и проведения работы по экспертизе ценности документов, включая управленческую, кадровую и иную коммерческую документацию, в том числе содержащую персональные данные, подготовки её к уничтожению или передаче в архивы на хранение в соответствии с требованиями Федерального законодательства. Экспертная комиссия является совещательным органом.

1.2. В своей деятельности экспертная комиссия руководствуется настоящим Положением, требованиями Федерального закона РФ от 27.07.2006 №152-ФЗ «О персональных данных», Постановления Правительства РФ от 15.09.2008 №687 «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.

1.3. Экспертная комиссия формируется распоряжением администрации Солигаличского муниципального округа Костромской области.

2. Функции экспертной комиссии

Экспертная комиссия организации осуществляет следующие функции:

2.1. Проводит заседания и рассматривает вопросы о порядке обработки в администрации Солигаличского муниципального округа Костромской области персональных данных и иной конфиденциальной информации; вопросы, регламентирующие порядок учёта, хранения и уничтожения материальных и электронных носителей информации ограниченного распространения.

2.2. Отбирает конфиденциальные документы организации (дела, журналы, книги) для проведения экспертизы ценности документов и принятия решения об их уничтожении либо дальнейшем хранении.

2.3. Представляет на утверждение главе Солигаличского муниципального округа Костромской области сводные описи дел постоянного и описей дел долговременного (свыше 10 лет) хранения, в том числе по личному составу.

2.4. Готовит протоколы заседания комиссии и акты о выделении к уничтожению документов по форме согласно приложению 1 и 2 к настоящему положению.

2.5. Осуществляет внутренний контроль за вопросами организации работы с документами, содержащими персональные данные, и соблюдением установленного режима их обработки.

2.6. Принимает непосредственное участие в подготовке ежегодной номенклатуры дел конфиденциального делопроизводства администрации Солигаличского муниципального округа Костромской области.

3. Права экспертной комиссии

Экспертной комиссии в процессе своей деятельности предоставляется право:

3.1. Консультировать работников, имеющих отношение к обработке персональных данных, по вопросам ведения конфиденциального делопроизводства, учёта документов и подготовки их к передаче в архив предприятия или уничтожения.

3.2. Осуществлять контроль и требовать от сотрудников администрации Солигаличского муниципального округа Костромской области:

- выполнения установленного порядка работы с документами, содержащими персональные данные;
- розыска отсутствующих дел, подлежащих передаче на хранение в архив;
- представления письменных объяснений по фактам утраты дел и документов.

3.3. Запрашивать от специалистов сведения и необходимые заключения для определения ценности документов и сроков их хранения.

3.4. Оказывать информационно-методическое содействие в вопросах обеспечения безопасности обрабатываемых в информационных системах сведений ограниченного распространения.

3.5. Информировать главу Солигаличского муниципального округа Костромской области о состоянии работы комиссии по рассматриваемым вопросам, входящим в сферу компетенции комиссии.

4. Организация работы экспертной комиссии

4.1. Экспертная комиссия осуществляет свою деятельность в непосредственном контакте с управляющим делами администрации муниципального округа, получая от него необходимые организационно-методические указания.

4.2. Вопросы, относящиеся к деятельности и компетенции комиссии, рассматриваются на её заседаниях, которые проводятся по мере необходимости.

4.3. Решения экспертной комиссии по рассматриваемым вопросам принимаются открытым голосованием большинством голосов.

4.4. Заседания комиссии протоколируются. Документирование работы комиссии и формирование дел с материалами её заседаний, возлагается на секретаря или одного из членов комиссии.

4.5. Акт комиссии утверждается главой Солигаличского муниципального округа Костромской области.

Приложение 1 к положению об экспертной комиссии администрации Солигаличского муниципального округа Костромской области

форма

ПРОТОКОЛ № ____
заседания экспертной комиссии

«___»_____ 201___ года г.Солигалич

Комиссия в составе:
председателя комиссии_____

секретаря комиссии _____
членов комиссии _____

_____

на очередном заседании рассмотрела следующие вопросы:

1. _____;
2. _____.

По первому вопросу слушали _____,

В ходе обсуждения данного вопроса были высказаны предложения о _____

Результаты голосования по первому вопросу: ЗА: - ___; ПРОТИВ: - 0 ; ВОЗДЕРЖАЛИСЬ: - 0.

Внесенные предложения были приняты к исполнению.

Секретарь комиссии: _____

«____»___20____ г.

Подписи: 1. _____
2. _____

Приложение 2 к положению об экспертной комиссии администрации Солигаличского муниципального округа Костромской области

Форма

Утверждаю:
Глава Солигаличского муниципального

округа Костромской области
«_____»_____20_____г.

АКТ №_____
о выделении к уничтожению документов, не подлежащих хранению

г.Солигалич «____»_____20__ года

На основании Перечня типовых управленческих документов, образующихся в деятельности госкомитетов, министерств, ведомств и других учреждений, организаций и предприятий с указанием сроков хранения, М. 1989 г., отобраны к уничтожению как не имеющие научно – исторической ценности и утратившие практическое значение документы фонда № 1 администрации Солигаличского муниципального округа Костромской области за период с _____ год.

№ п/п	Заголовок дела или групповой заголовок документов	Крайние даты	Номера описей	Индекс дела по номенклатуре или номер ед.хр. по описи	Количество ед. хр.	Срок хранения, номера статей по перечню	Примечание
1	2	3	4	5	6	7	8

Итого_____ ед. хр. за _____ год(ы).
(цифрами и прописью)

Описи дел постоянного хранения за _____ годы утверждены.

Документам с отметкой ЭПК проведена полистовая экспертиза, на постоянное хранение документы не отложились.

Экспертизу ценности документов провела:

_____ _____ _____
(должность) (подпись) (ФИО)
«____»_____20__ г.

СОГЛАСОВАНО
Протокол заседания экспертной комиссии администрации Солигаличского муниципального округа Костромской области от _____20___ г. №_____

Документы сданы
_____
(наименование организации)
на переработку по приемо-сдаточной накладной _____ № _____
(дата)

_____ _____ _____
(должность) (подпись) (ФИО)
«____»_____20__ г.

Изменения в учетные документы внесены.

_____ _____ _____
(должность) (подпись) (ФИО)

«____»_____20__ г.

Приложение № 17 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

ПОЛОЖЕНИЕ
об обработке конфиденциальной информации
в администрации Солигаличского муниципального округа Костромской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке конфиденциальной информации в администрации Солигаличского муниципального округа Костромской области (далее - Положение) регулирует в соответствии Федеральными законами Российской Федерации от 29 июля 2004 года N 98-ФЗ "О коммерческой тайне", от 27 июня 2006 года N 149-ФЗ "Об информации, информационных технологиях и защите информации", от 27 июля 2006 года N 152-ФЗ "О персональных данных", Постановлением Правительства от 15 сентября 2008 года N 687 "Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", иными федеральными законами и нормативными правовыми актами Российской Федерации отношения, связанные с охраной и использованием конфиденциальной информации в администрации Солигаличского муниципального округа Костромской области (далее - администрация муниципального округа).

1.2. Сведения о лицах (данные персонального характера), предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления и существования, отнесенные к конфиденциальной информации в соответствии с "Перечнем сведений ограниченного распространения" (Приложение к Положению), имеющие действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам и ограничения по доступу, регламентированные федеральным законодательством, подлежат защите от несанкционированного доступа при их обработке в подразделениях администрации муниципального округа.

1.3. Администрация Солигаличского муниципального округа Костромской области имеет исключительное право на использование конфиденциальной информации, составляющей её коммерческую и служебную тайны, любыми не запрещенными законом способами по собственному усмотрению.

1.4. В соответствии с настоящим Положением администрация Солигаличского муниципального округа Костромской области принимает меры к охране конфиденциальной информации различными способами, в том числе с использованием организационно-распорядительных, правовых, технических и криптографических мер, позволяющих ограничивать доступ к ней третьих лиц.

1.5. Целью охраны конфиденциальной информации является обеспечение экономической и правовой безопасности администрации муниципального округа.

1.6. В случае если в связи с осуществлением своей деятельности работникам Солигаличского муниципального округа Костромской области становятся известными сведения, составляющие в соответствии с законодательством Российской Федерации государственную тайну, администрация муниципального округа обязана предпринимать меры по их охране в соответствии с Федеральным законом Российской Федерации от 21 июля 1993 года N 5485-1"О государственной тайне" и иными нормативными правовыми актами о государственной тайне.

1.7. Действие настоящего Положения распространяется на структурные подразделения администрации Солигаличского муниципального округа Костромской области.

2. КОММЕРЧЕСКАЯ ТАЙНА

2.1. Коммерческая тайна администрации Солигаличского муниципального округа Костромской области - информация, позволяющая её обладателю при существующих или

возможных обстоятельствах обеспечивать исполнение возложенных законодательством функций и услуг с наименьшими бюджетными затратами.

Перечень сведений, являющихся коммерческой тайной администрации муниципального округа, определяется "Перечнем сведений ограниченного распространения", который утверждается администрацией муниципального округа (Приложение к Положению).

2.2. К коммерческой тайне могут быть отнесены любые сведения, за исключением той информации, которая в соответствии с законодательством не может быть отнесена к коммерческой тайне.

2.3. В соответствии с законодательством к коммерческой тайне не может быть отнесена следующая информация:

2.3.1. Учредительные документы;

2.3.2. Регистрационные удостоверения, лицензии, патенты и иные документы, дающие право заниматься тем или иным видом деятельностью;

2.3.4. Документы о платежеспособности;

2.3.5. Сведения о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

2.3.6. Документы об уплате налогов и обязательных платежах;

2.3.7. Сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства Российской Федерации и размерах причиненного при этом ущерба, в случае если данные факты установлены вступившим в законную силу решением (приговором) суда, арбитражного суда;

2.3.8. Идентификационный номер налогоплательщика (ИНН);

2.3.9. Содержание внешней бухгалтерской отчетности, в том числе содержание: бухгалтерского баланса; отчета о прибылях и убытках; приложений к ним, предусмотренных нормативными актами; аудиторского заключения, подтверждающего достоверность бухгалтерской отчетности; пояснительной записки к данным внешней бухгалтерской отчетности;

2.3.11. Иная информация, которая не может быть отнесена к коммерческой тайне в соответствии с федеральным законодательством Российской Федерации.

2.4. Отнесение информации, указанной в "Перечне сведений ограниченного распространения" к информации, составляющей коммерческую тайну администрации муниципального округа, не требует издания каких-либо иных актов помимо настоящего Положения.

2.5. Отнесение информации, указанной в пункте 2.2. настоящего Положения, к информации, составляющей коммерческую тайну, осуществляется путём издания в каждом конкретном случае постановления администрации муниципального округа и обязательного включения информации в "Перечень сведений ограниченного распространения".

Инициатива в издании постановления администрации муниципального округа об отнесении той или иной информации к коммерческой тайне может исходить от руководителей структурных подразделений.

2.6. К коммерческой тайне не относится информация, разглашённая администрацией муниципального округа самостоятельно или с её согласия.

3. СЛУЖЕБНАЯ ТАЙНА

3.1. Служебную тайну администрации Солигаличского муниципального округа Костромской области составляют любые сведения, в том числе сведения, которые могут содержаться в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных и иных сообщениях, передаваемых по сетям электрической и почтовой связи и которые стали известны работнику администрации Солигаличского муниципального округа Костромской области в связи с исполнением им возложенных на него трудовых обязанностей (Приложение к Положению).

3.2. К служебной тайне не относится информация, разглашенная должностными лицами администрации Солигаличского муниципального округа Костромской области с согласия

администрации Солигаличского муниципального округа Костромской области, а также иная информация, ограничения доступа к которой не допускаются в соответствии с законодательством Российской Федерации.

4. ПЕРСОНАЛЬНЫЕ ДАННЫЕ

4.1. Персональные данные - это любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

4.2. В соответствии со ст.7 Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" персональные данные относятся к информации ограниченного распространения (конфиденциальной информации).

4.3. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральными законами.

4.4. Перечень сведений персонального характера, обрабатываемых в администрации Солигаличского муниципального округа Костромской области, указан в Приложении к настоящему Положению.

5. ОХРАНА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

5.1. Охрана конфиденциальной информации (персональные данные, коммерческая и служебная тайна) состоит в принятии комплекса режимных, правовых, технических и криптографических мер, направленных:

- на ограничение доступа к обрабатываемым персональным данным, коммерческой и служебной тайне (далее конфиденциальной информации) третьих лиц;
- на предотвращение несанкционированного разглашения конфиденциальной информации;
- на выявление нарушений режима конфиденциальности информации;
- на пресечение нарушений режима конфиденциальности информации;
- на привлечение лиц, нарушающих режим конфиденциальности информации к установленной законодательством ответственности.

5.2. При приеме на работу нового работника руководитель структурного подразделения администрации муниципального округа в соответствии с предполагаемой должностью определяет уровень его доступа к конфиденциальной информации.

Исходя из этого, при заключении трудового договора, работники, которые в силу своих служебных обязанностей будут иметь отношение к обработке конфиденциальной информации, дают письменное обязательство о соблюдении режима конфиденциальности, установленного в администрации муниципального округа.

5.3. Каждый работник при приеме на работу проходит инструктаж о существующем режиме конфиденциальности, знакомится под роспись в листе ознакомления с Положением, регламентирующим порядок обработки конфиденциальной информации, Перечнем сведений, составляющим коммерческую и служебную тайну и предупреждается об ответственности за нарушение существующего режима.

5.4. Заключаемые администрацией Солигаличского муниципального округа Костромской области договоры, предполагающие обмен или передачу информации ограниченного распространения, должны содержать обязательное условие о сохранении Сторонами режима конфиденциальности.

5.5. В рабочих и иных помещениях административного здания администрации Солигаличского муниципального округа Костромской области создаются условия, ограничивающие доступ к конфиденциальной информации третьих лиц и несанкционированное её разглашение, в том числе устанавливаются технические средства защиты от несанкционированного доступа к местам хранения документов (сейфы и металлические ящики) и информации (программные и аппаратные средства защиты).

5.6. Администрация Солигаличского муниципального округа Костромской области предпринимает необходимые меры по выявлению фактов нарушения режима конфиденциальности и пресечению выявленных нарушений режима конфиденциальной

информации всеми допустимыми способами, в том числе регламентацией технологических процессов обработки персональных данных и иной конфиденциальной информации.

5.7. Лица, виновные в нарушении режима конфиденциальности информации, привлекаются к установленной законодательством ответственности.

6. ПОРЯДОК ИСПОЛЬЗОВАНИЯ И ПРЕДОСТАВЛЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

6.1. К обработке конфиденциальной информации допускаются только те сотрудники администрации Солигаличского муниципального округа Костромской области, которым доступ к такой информации необходим и разрешён в силу выполняемых ими функций.

6.2. Предоставление конфиденциальной информации третьим лицам возможно не иначе как с разрешения главы Солигаличского муниципального округа Костромской области.

6.3. В части, касающейся порядка предоставления персональных данных работников и должностных лиц контрагентов, с которыми установлены договорные отношения, а также иной конфиденциальной информации, обладатель таких сведений руководствуется требованиями установленного в администрации муниципального округа режима конфиденциальности и положениями федеральных законов.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Лица, виновные в нарушении режима конфиденциальной информации, привлекаются в установленном порядке к уголовной, административной, дисциплинарной и гражданско-правовой ответственности.

7.2. Во всём ином, что не урегулировано настоящим Положением, применяются положения действующего законодательства Российской Федерации.

Приложение к положению об обработке конфиденциальной информации администрации Солигаличского муниципального округа Костромской области

ПЕРЕЧЕНЬ СВЕДЕНИЙ
ограниченного распространения в администрации Солигаличского муниципального округа Костромской области (конфиденциальная информация)

1. ОБЩИЕ ПОЛОЖЕНИЯ

Данный перечень сведений ограниченного распространения ограниченного распространения в администрации Солигаличского муниципального округа Костромской области (конфиденциальная информация) (далее - Перечень) разработан в целях регулирования отношений, связанных с владением, хранением и обработкой конфиденциальной информации (персональные данные, служебная и коммерческая тайна) в процессе осуществления управленческой, финансовой и производственной деятельности в администрации Солигаличского муниципального округа Костромской области (далее - администрация муниципального округа).

При подготовке Перечня учитывались требования Федеральных законов от 29 июля 2004 года N 98-ФЗ "О коммерческой тайне", от 27 июля 2006 года N 152-ФЗ "О персональных данных", Постановления Правительства РСФСР от 05 декабря 1991 года N 35 "О перечне сведений, которые не могут составлять коммерческую тайну", ст.139 Гражданского кодекса Российской Федерации и Указа Президента Российской Федерации от 06 марта 1997 года N 188 "Перечень сведений конфиденциального характера".

Основные термины и определения, используемые при регулировании отношений, связанных с владением конфиденциальной информации:

персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

коммерческая тайна - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

обладатель конфиденциальной информации - физическое или юридическое лицо, занимающееся предпринимательской деятельностью, правомерно владеющее информацией, охраняемом законом, имеющей действительную или потенциальную коммерческую ценность и ограничивающее доступ к этой информации на законном основании либо принимающее меры к охране ее конфиденциальности;

доступ к конфиденциальной информации - ознакомление определенных лиц при условии сохранения конфиденциальности с информацией, составляющей коммерческую и иные тайны, с согласия обладателя или на ином установленном законом основании;

передача конфиденциальной информации - доведение обладателем коммерческой тайны зафиксированной на материальных носителях информации, составляющей эту коммерческую тайну, до определенных лиц и принятие ими установленных законом или договором мер по охране ее конфиденциальности;

режим конфиденциальности - установленный в администрации муниципального округа комплекс правовых, организационных, технических и иных мер, применяемый к режиму обработки информации ограниченного распространения как обладателем этой информации, так и лицами, правомерно ее получившими;

разглашение конфиденциальной информации - деяние (действие или бездействие), в результате которого информация, составляющая коммерческую и иные тайны, становится известной (раскрытой) третьим лицам без согласия обладателя этих тайн, а также вопреки трудовому или гражданско-правовому договору.

2. СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, ОТНОСИМЫЕ К ПЕРСОНАЛЬНЫМ ДАННЫМ

Категория сведений	Характеристика	Обладатель ПД
2.1. Персональные данные Работников		
Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу	По каждому субъекту персональных данных	Глава округа, заместители главы администрации, управляющий делами, руководители структурных подразделений администрации
2.2. Дополнительные сведения о Работниках		
Сведения о больничных листах, отчислениях в ПФР, ФСС и т.д.	По каждому субъекту персональных данных	Глава округа, заместители главы администрации, управляющий делами, руководители структурных подразделений администрации
Сведения о начислениях заработной платы, командировочных расходах, отпускных и др. финансовых показателях	По каждому субъекту персональных данных	Глава округа, заместители главы администрации, управляющий делами, руководители структурных подразделений администрации
2.3. Кандидаты на работу		
Сведения о субъектах персональных данных, рассматриваемых в качестве кандидатов на работу, отраженные в Анкете кандидата	По каждому субъекту персональных данных	Глава округа, заместители главы администрации, управляющий делами, руководители структурных подразделений

		администрации, члены конкурсной комиссии на замещение вакантных должностей муниципальной службы
2.4. Контрагенты		
Сведения о должностных лицах государственных и муниципальных учреждений, юридических лицах, индивидуальных предпринимателях, с которыми установлены договорные отношения	Общедоступные данные (субъекты Договорных отношений)	Глава округа, заместители главы администрации, управляющий делами, руководители структурных подразделений администрации
2.5. Граждане		
Сведения персонального характера об обратившихся в администрации муниципального округа	По каждому субъекту ПДн	Глава округа, заместители главы администрации, управляющий делами, руководители структурных подразделений администрации, главный специалист – ответственный секретарь комиссии по делам несовершеннолетних и защите их прав
2.6. Безопасность		
Сведения о местах хранения документов и материалов, содержащих персональные данные работников, и порядке доступа к ним	В объеме администрации муниципального округа	Глава округа, заместители главы администрации, управляющий делами, руководители структурных подразделений администрации
Сведения о порядке и состоянии режима охраны и существующей системы охранной сигнализации	В объеме администрации муниципального округа	Глава округа, заместители главы администрации, управляющий делами, руководители структурных подразделений администрации
Сведения, об используемой системе защиты персональных данных в организации и принимаемых мерах по обеспечению безопасности обрабатываемой информации	В объеме администрации муниципального округа	Глава округа, заместители главы администрации, управляющий делами, руководители структурных подразделений администрации

3. СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, ОТНОСИМЫЕ К КОММЕРЧЕСКОЙ ТАЙНЕ

Категория сведений	Характеристика	Обладатель КТ
3.1. ФИНАНСЫ		
Сведения о кругообороте средств организации, финансовых операциях, (состоянии банковских счетов организации и проводимых операциях, об уровне доходов организации, о состоянии кредита организации,	В объеме администрации муниципального округа	Глава округа, заместители главы администрации, финансовое управление администрации

пассивы и активы). Главная книга организации		
3.2. ПЛАНИРОВАНИЕ		
Сведения о планах расширения или свертывания различных видов оказываемых услуг и их экономических обоснованиях	В объеме администрации муниципального округа	Глава округа, заместители главы администрации, отдел по экономическому развитию, строительству и архитектуре администрации
Сведения о планах инвестиций, закупок и продаж	В объеме администрации муниципального округа	Глава округа, заместители главы администрации, финансовое управление администрации, отдел по экономическому развитию, строительству и архитектуре администрации

4. СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, ОТНОСИМЫЕ К СЛУЖЕБНОЙ ТАЙНЕ

Категория сведений	Характеристика	Обладатель КТ
4.1. БЕЗОПАСНОСТЬ		
Сведения, раскрывающие систему безопасности и используемые технические средства защиты конфиденциальной информации, обрабатываемой в автоматизированной информационной системе (АИС)	В объеме администрации муниципального округа	Глава округа, заместители главы администрации, руководители структурных подразделений, лица, допущенные к работе на объекте информатизации
Сведения о порядке организации допуска пользователей к информационным ресурсам ограниченного распространения, обрабатываемым в АИС, в том числе к ПДн	В объеме администрации муниципального округа	Лица, имеющие допуск к работе на объекте информатизации
Сведения о действующих в АИС учётных записях (логин+пароль)	В объеме единичной записи	Лица, имеющие допуск к работе на объекте информатизации
Документация на объект информатизации	Протоколы испытаний, Инструкции, Предписание на эксплуатацию и технический паспорт АС	Лица, имеющие допуск к работе на объекте информатизации
Информация о значениях закрытых ключей	В объеме единичного значения	Пользователи СКЗИ
Файлы запроса на изготовление сертификатов открытых ключей в электронной форме	В объеме единичного запроса	Пользователи СКЗИ

5. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ

5.1. За незаконный сбор, разглашение или использование конфиденциальной информации (персональные данные, коммерческая или служебная тайна) организации, в соответствии с законодательством Российской Федерации наступает дисциплинарная, гражданско-правовая, административная или уголовная ответственность.

5.2. В случае причинения убытков обладателю коммерческой или служебной тайны в результате нарушения его прав эти убытки подлежат возмещению в размере, определяемом при рассмотрении материалов в суде.

Приложение № 18 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Перечень информационных систем персональных данных, используемых в администрации Солигаличского муниципального округа Костромской области

Информационные системы
Сайт администрации Солигаличского муниципального округа Костромской области http//soligalich.org
РСМЭВ - Региональная система межведомственного электронного взаимодействия Костромской области
ИС «Сбербанк онлайн»
СЭДД «Lotus»
ИС «Контур-Экстерн»

Приложение № 19 к постановлению администрации Солигаличского муниципального округа Костромской области от 27 марта 2024 года № 367

Правила
работы с информационными системами администрации Солигаличского муниципального округа Костромской области

1. Общие положения

1.1. Настоящие Правила определяют основные принципы безопасной работы автоматизированных информационных систем администрации Солигаличского муниципального округа Костромской области и обработки конфиденциальной информации работниками администрации Солигаличского муниципального округа Костромской области – (далее - администрация муниципального округа).

1.2. Целью данного документа является формализация требований, предъявляемых к сотрудникам по обеспечению режима безопасности конфиденциальной информации, циркулирующей в информационных системах, в том числе при обработке персональных данных.

1.3. Правила разработаны в соответствии с требованиями Федеральных законов РФ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 №152-ФЗ «О персональных данных», постановлений Правительства РФ от 01.11.2012 №1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и иных нормативных актов.

2. Основные термины и определения

Автоматизированное рабочее место пользователя (далее АРМ) - персональный компьютер с предустановленным системным, прикладным и антивирусным программным обеспечением (далее ПО), в том числе предназначенным для защиты информации ограниченного распространения.

Информационная система персональных данных (далее ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Информационные ресурсы - программное обеспечение, документы и массивы документов расположенные, хранящиеся и обрабатываемые в информационных системах;

Интернет - всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных (телекоммуникационная сеть общего пользования);

Пользователь - сотрудник, допущенный к работе на автоматизированном рабочем месте и использующий для исполнения своих должностных обязанностей средства вычислительной техники;

Персональный компьютер (далее ПК) - компьютер, с предустановленным системным, прикладным и антивирусным ПО и предназначенный для эксплуатации одним пользователем, то есть для личного использования;

Электронная почта - технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети;

Flash-карта - разновидность твердотельной полупроводниковой энергонезависимой перезаписываемой памяти (один из видов электронных носителей информации).

3. Общие правила работы на АРМ

3.1. В целях исполнения своих служебных обязанностей, сотруднику администрации муниципального округа (пользователю) на период работы предоставляется автоматизированное рабочее место с предустановленным лицензионным системным, прикладным и антивирусным программным обеспечением, имеющим сертификаты соответствия по безопасности.

Для организации доступа пользователя к информационным ресурсам АИС его АРМ подключается к локальной вычислительной сети (далее ЛВС). Установку и настройку АРМ, а также подключение ПК к ЛВС выполняет Администратор безопасности.

Также Администратор безопасности проводит опечатывание ПК. Информация об опечатывании вносится в Журнал опечатывания системных блоков (Приложение 2 к правилам работы с информационными системами Солигаличского муниципального округа Костромской области).

3.2. Допуск пользователя к АРМ осуществляется по устной заявке начальнику отдела информационно-технического обеспечения администрации муниципального округа (либо его заместителю) на основании утвержденного Перечня должностей, имеющих право доступа к обработке конфиденциальной информации, в том числе персональных данных.

Доступ пользователя к работе на АРМ осуществляется на основании индивидуальной учетной записи (Логин + Пароль). Пользователь обязан использовать пароль в соответствии со следующими требованиями:

- длина пароля должна быть не менее 8 символов;

- пароль не должен быть легко угадываемым (не должен включать повторяющуюся последовательность каких-либо символов (например, "11111111", "абвгдеё" и т.п.), пароль не должен включать в себя легко подбираемые сочетания символов (имена, фамилии, даты рождения знакомых, наименования городов и улиц, клички домашних животных и т.п.), а также общепринятые сокращения (ЭВМ, ЛВС и т.п.).

- пароли вносятся в журнал выдачи парольных карточек (Приложение 3 к правилам работы с информационными системами Солигаличского муниципального округа Костромской области).

3.3. Пользователь обеспечивает безопасное хранение пароля, исключающее возможность его утери или разглашения. Срок использования пароля составляет не более 6 мсяцев. При смене пароля новое значение должно отличаться от предыдущего не менее чем в трёх-четырёх позициях.

3.4. При необходимости оставить рабочее место, даже на короткое время, пользователь должен заблокировать доступ к АРМ, нажав одновременно Ctrl + Alt + Delete, и принять иные меры по ограничению доступа к отображаемой на экране монитора информации

3.5. При использовании телекоммуникационных возможностей сети общего пользования Интернет пользователи обязаны выполнять следующие требования:

- использовать ресурсы Интернет только для выполнения своих служебных обязанностей;

- не посещать ресурсы Интернет, содержащие материалы противозаконного, экстремистского или неэтичного характера, а также использовать доступ к социальным сетям Интернет и развлекательным сайтам;

- не размещать в сети Интернет информацию служебного характера, о её сотрудниках и решаемых задачах, если это не связано с выполнением служебных обязанностей; - не использовать Интернет для несанкционированной передачи (выгрузки) или получения (загрузки) видео-, аудио- и информационных материалов, защищенных авторским правом;

3.6. При работе с электронной почтой пользователи должны соблюдать следующие требования:

- запрещается использовать возможности электронной почты для отправки сообщений противозаконного (террористического, экстремистского или враждебного характера), а также содержащего в себе информацию неэтичного содержания;

- при получении электронных сообщений из незнакомого источника и/или сомнительного содержания не следует открывать файлы, вложенные в сообщение, так как они с большой долей вероятности могут содержать вирусы. Такие сообщения необходимо удалять;

-не отвечать на подозрительные письма и, тем более, сообщать любые данные о себе и сотрудниках.

3.7. По окончании рабочего времени при отсутствии служебной необходимости пользователь обесточивает АРМ и другую оргтехнику во избежание выхода её из строя и в целях обеспечения противопожарной безопасности.

3.8. В случае подозрения на компрометацию пароля доступа необходимо немедленно изменить пароль и проинформировать об этом своего непосредственного руководителя.

В процессе эксплуатации АРМ пользователям ЗАПРЕЩАЕТСЯ:

3.9. Открывать корпус системного блока и вносить изменения в конфигурацию ПК;

3.10. Без получения санкции руководителя и администратора безопасности изменять настройки программного обеспечения и параметры доступа к информационным ресурсам;

3.11. Отключать и изменять параметры настройки в установленное антивирусное программное обеспечение и иные средства защиты информации;

3.12. Подключать к АРМ неучтенные внешние запоминающие устройства (активное сетевое оборудование, незарегистрированные Flash-карты. НЖМД, смартфоны, фотоаппараты и т.д.), если это не связано с исполнением должностных обязанностей сотрудника;

3.13. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты для организации несанкционированного доступа к обрабатываемым информационным ресурсам. При обнаружении такого рода ошибок необходимо информировать своего непосредственного руководителя и администратора безопасности;

3.14. Осуществлять действия направленные на преодоление систем безопасности, получение несанкционированного доступа к ресурсам информационной сети и перехват информации, циркулирующей в ИС;

3.15. Оставлять оборудование АРМ, переносные компьютеры и средства хранения информации без личного присмотра, в случаях, если это может привести к их краже;

При наличии риска хищения ПК и (или) средств хранения информации, необходимо принять меры по их минимизации (например, убирать переносной компьютер на обеденный перерыв и после завершения рабочего дня в закрывающийся на ключ шкаф, не оставлять

незакрытым помещение, в котором находится оборудование информационной системы, использовать замки для переносных компьютеров);

3.16. Осуществлять обработку конфиденциальной информации на ПК, не оснащенном принятыми в администрации средствами защиты информации, а также в присутствии лиц, не имеющих права доступа к данной информации, если при этом указанные лица могут ознакомиться с обрабатываемой информацией;

3.17. Записывать и хранить конфиденциальную информацию на неучтённых носителях информации (Flash-карта, CD-диск, носимый HDD и т.п), а также оставлять без личного присмотра на рабочем месте или где бы то ни было носители информации и распечатки, содержащие подобную информацию;

3.18. Допускать к работе на ПК лиц, не имеющих прав доступа к информационным ресурсам.

4. Порядок работы с информационной системой

4.1. При работе с программными и техническими средствами, входящими в состав АРМ и информационной системы, пользователь обязан выполнять установленные правила их эксплуатации. За неисполнение установленных правил он несёт персональную ответственность.

4.2. Администрация муниципального округа оставляет за собой право протоколировать и контролировать действия сотрудников при обработке конфиденциальной информации, обрабатываемой в информационной системе.

4.3. Пользователи не имеют права предпринимать попыток получения доступа к закрытым информационным ресурсам, не получив официального разрешения на доступ к ним.

4.4. Пользователи не должны разглашать сведения о содержании информации, ставшей известной им в ходе выполнения должностных обязанностей, а также о процедурах и технической реализации защиты информации.

4.5. В целях повышения эффективности служебной деятельности для обмена открытыми информационными ресурсами (обновления программных продуктов, инструкции, правила и т.п.) между пользователями могут использоваться съёмные материальные носители информации (Flash-карты, переносные жесткие диски, иные устройства записи и чтения), зарегистрированные и учтённые по Журналу учёта съемных носителей информации.

4.6. Выдача сотрудникам и учёт материальных носителей информации осуществляется сотрудником, ответственным за организацию работы по защите персональных данных, по Журналу учёта съёмных носителей информации.

5. Ответственность за нарушение порядка

5.1. Ответственность за неисполнение требований настоящей Инструкции возлагается на всех сотрудников, являющихся пользователями информационной системы администрации.

5.2. Сотрудник, нарушивший требования данной Инструкции, может быть подвергнут дисциплинарному наказанию в соответствии с законодательством Российской Федерации.

Приложение 1 к правилам работы с информационными системами Солигаличского муниципального округа
Костромской области

Журнал опечатывания системных блоков

п\п	Отдел	Инвентарный номер	№ стикера	Дата опечатывания	Дата снятия печати	Подпись ответственного лица

Приложение 2 к правилам работы с информационными системами

Солигаличского муниципального округа
Костромской области

Журнал выдачи парольных карточек

	Пароль	Парольная фраза	Дата получения	Пользователь (подпись, расшифровка)

Приложение 3 к правилам работы с информационными системами Солигаличского муниципального округа Костромской области

Инструкция администратора безопасности автоматизированных информационных систем

1. Общие положения

1.1. Настоящая Инструкция разработана на основании действующих нормативных документов и определяет общие функции, права и обязанности администратора безопасности по вопросам обеспечения информационной безопасности при обработке персональных данных и иной конфиденциальной информации с использованием средств автоматизации, входящих в состав автоматизированных информационных систем (далее – АИ С)

1.2. Администратор безопасности (далее - Администратор) в своей работе руководствуется настоящей Инструкцией, внутренними нормативными документами и требованиями законодательства в сфере защиты информации ограниченного доступа.

1.3. Администратор безопасности назначается из числа сотрудников Оператора персональных данных, имеющих соответствующую квалификацию и опыт работы с оборудованием и программным обеспечением информационных систем. Администратор безопасности является ответственным должностным лицом организации и обеспечивает правильное использование и функционирование установленного системного и прикладного программного обеспечения, средств технической защиты информации (далее по тексту - СЗИ) от несанкционированного доступа (далее по тексту - НСД), а также поддержание достигнутого уровня защиты АИС и её ресурсов на этапах эксплуатации и модернизации.

1.4. Администратор безопасности имеет рабочее место, размещаемое в выделенном помещении, оборудованном средствами физической защиты в которое исключается несанкционированный доступ посторонних лиц. Рабочее место Администратора подключается к ЛВС, оборудуется средствами удаленного контроля используемых информационных ресурсов и местами хранения конфиденциальных документов.

1.5. Требования Администратора безопасности к сотрудникам, связанные с выполнением ими своих должностных обязанностей, обязательны для исполнения всеми пользователями АИС.

1.6. Администратор безопасности осуществляет плановый и периодический контроль действий пользователей при работе в АИС, определяет текущее состояние и поддерживает установленный уровень защиты конфиденциальной информации.

2. Администратор безопасности в своей деятельности имеет право:

2.1. Знать и выполнять требования действующих в организации нормативных и руководящих документов по защите информации, а также внутренних Инструкций регламентирующих работу с конфиденциальной информацией.

2.2. Оказывать содействие в установке и настройке автоматизированных рабочих мест сотрудников администрации, а также осуществлять сопровождение работы установленного системного и прикладного программного обеспечения и средств защиты информации.

2.3. Организовывать доступ пользователей к ресурсам автоматизированной информационной системы в соответствии с Перечнем должностей, имеющих право доступа к обработке конфиденциальной информации, на основании письменных заявок, утверждаемых руководителем организации.

2.4. Уточнять в установленном порядке обязанности пользователей ИС при обработке на автоматизированном рабочем месте (АРМ) конфиденциальных сведений, в том числе персональных данных, являющихся объектами защиты.

2.5. Осуществлять резервное копирование критичных для работы администрации информационных ресурсов, обеспечивая их защиту и целостность.

2.6. Принимать участие в реализации плановых мероприятий по защите конфиденциальной информации, в том числе персональных данных, циркулирующих в АИС.

2.7. Оказывать помощь пользователям ИСПДн в части консультирования по вопросам введенного режима защиты персональных данных.

2.8. Анализировать состояние принятых в организации мер защиты конфиденциальной информации, в том числе выявлять попытки несанкционированного доступа к ресурсам ИС и совершенствовать методы защиты от угроз информационной безопасности.

2.9. Вести журнал учёта событий, регистрируемых средствами защиты, с целью выявления возможных нарушений или попыток несанкционированного доступа.

2.10. Своевременно вносить коррективы в список пользователей информационных ресурсов и матрицу доступов к персональным данным при приеме на работу и увольнении сотрудников. Удалять учётные записи пользователей ИС на доступ к информационным ресурсам в течение суток после подписания Обходного листа либо получения информации от руководителей подразделений об увольнении сотрудника.

2.11. В соответствии с планом внутренних проверок состояния обработки и защиты конфиденциальной информации в том числе персональных данных, на регулярной основе осуществлять контроль:

- за соблюдением сотрудниками требований действующих нормативных и руководящих документов, регламентирующих обработку конфиденциальной информации; - за осуществлением неизменности и целостности программной среды АИС (системное и прикладное ПО), средств антивирусной защиты и межсетевого экранирования, их параметров и режимов;

- за наличием и возможным использованием на автоматизированных рабочих местах вредоносных программ и иного нелицензионного ПО, не связанного с выполнением функциональных задач;

- за соблюдением пользователями принятого в организации режима парольной политики и порядка использования учётных записей на доступ к информационным ресурсам;

- за состоянием допуска пользователей к работе с ресурсами АИС и изменением прав доступа к защищаемой конфиденциальной информации, в том числе персональным данным;

- за выполнением правил учёта, использования и хранения электронных носителей конфиденциальной информации;

- за соблюдением сроков смены паролей доступа к ресурсам АИС и выполнением рекомендаций по выбору наиболее безопасных Паролей;

- за поддержанием установленного порядка обновления антивирусных баз и антивирусной защиты информационных ресурсов;

- за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусах системных блоков АРМ, обрабатывающих информацию ограниченного доступа; - за сроками действия сертификатов и лицензий эксплуатируемого оборудования и ПО;

2.12. В случаях отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты, принимать меры по своевременному восстановлению и выявлению причин, приведших к отказу работоспособности, а также недопущения доступа посторонних лиц к конфиденциальной информации.

2.13. Периодически информировать руководство о состоянии защиты конфиденциальной информации, о нештатных ситуациях на объектах АИС, о работе сотрудников в сетях общего пользования, в том числе в Интернет, и допущенных пользователями нарушениях требований по защите информации, предусмотренных руководящими документами.

3. Администратор безопасности обязан:

3.1. Принимать необходимые меры по обеспечению безаварийного функционирования и работоспособности автоматизированных средств обработки информации, системного и прикладного ПО, СЗИ от НСД в пределах, возложенных на него функций;

3.2. Проводить инструктаж пользователей правилам работы на АРМ, с установленными СКЗИ и СЗИ от НСД;

3.3. Докладывать главе администрации или лицу, исполняющему его обязанности, о фактах и попытках несанкционированного доступа к конфиденциальной информации, о неправомерных действиях пользователей или иных лиц, приводящих к нарушению требований безопасности информации.

3.5. Вносить изменения в документацию ИС в соответствии с требованиями нормативных документов в части, касающейся СЗИ от НСД;

3.6. Проводить работу по выявлению возможных каналов утечки конфиденциальной информации, вести их учёт и принимать меры к их устранению;

3.7. Регистрировать факты нарушений требований режима безопасности и организовывать проведение расследований по возникшим инцидентам информационной безопасности.

3.8. Блокировать учётные записи пользователей на АРМ в случае окончания срока действия сертификата соответствия ФСТЭК России, ФСБ России на любое СЗИ, из используемых в ИСПДн, до момента его продления. В случае непродления сертификата соответствия на СЗИ администратор обязан поставить в известность орган по аттестации, проводивший аттестацию ИСПДн, для принятия дальнейшего совместного решения.

3.9. Контролировать действия пользователей при уничтожении и затирании информации записанной на электронных носителях (накопителях) информации.

4. Администратор безопасности имеет право:

4.1. Запрашивать и получать необходимую информацию от структурных подразделений администрации муниципального округа для планирования и организации работ по защите конфиденциальной информации.

4.2. Требовать от сотрудников администрации муниципального округа - пользователей ИСПДн соблюдения установленных технологий обработки информации и выполнения требований руководящих документов.

4.3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, доступа к информационным ресурсам, утраты, порчи защищаемой информации и технических компонентов автоматизированной системы.

4.4. Требовать от руководителей структурных подразделений администрации муниципального округа прекращения работы сотрудников в автоматизированной информационной системе при несоблюдении ими установленной технологии обработки информации или невыполнения требований по безопасности.

4.5. Вносить на рассмотрение руководства предложения по совершенствованию технических мер защиты.

5. Администратор безопасности несёт ответственность:

5.1. За разглашение конфиденциальных сведений организации (в том числе - персональных данных работников и должностных лиц контрагентов, используемых способов и методов защиты информационных ресурсов), ставших ему известными по роду своей деятельности.

5.2. За умышленное причинение материального ущерба, повлекшее отказ в работе оборудования корпоративной информационной системы, - в пределах, определенных действующим трудовым, уголовным и гражданским законодательством РФ.

Приложение 4 к правилам работы с информационными системами

Солигаличского муниципального округа
Костромской области

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
пользователя информационной системы персональных данных администрации Солигаличского муниципального округа Костромской области

Настоящая инструкция разработана в рамках выполнения работ по обеспечению безопасного администрирования информационных систем, обрабатывающих персональные данные в администрации Солигаличского муниципального округа (далее – ИСПДн).

1. Общие положения

1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных администрации Солигаличского муниципального округа Костромской области (далее – администрация муниципального округа).

1.2. Пользователями являются работники администрации муниципального округа, определенные Перечнем должностей сотрудников, имеющих доступ к персональным данным работников администрации Солигаличского муниципального округа Костромской области и которым они необходимы в связи с исполнением трудовых обязанностей , участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющих 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 Федеральными законами от 06.10.2003 года № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», от 27 июля 2006 г. № 252-ФЗ «О персональных данных», Постановлением Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативно правовыми актами, операторами, являющимися государственными или муниципальными органами», Уставом муниципального образования Солигаличский муниципальный район Костромской области, Положением о защите персональных данных работников администрации Солигаличского муниципального округа, Костромской области настоящей инструкцией.

1.5. Методическое руководство работой пользователя осуществляется Администратором ИСПДн.

2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования настоящей инструкции и других внутренних распоряжений, регламентирующих порядок действий по защите персональных данных.

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

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 3).

2.5. Соблюдать правила при работе в сетях общего доступа, Интернет и других (раздел 4).

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

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2.8. Пользователям 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;

- 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 на-стройки АРМ, без согласования с Администратором ИСПДн;

2.9. 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>

2.10. Принимать меры по реагированию, в случае возникновения вне-штатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий в пределах возложенных на него функций.

3. Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользовате-лям Администратором ИСПДн или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 6 месяцев.

3.3. Правила формирования пароля:

- Пароль не может содержать имя учетной записи пользователя или ка-кую-либо его часть.

- Пароль должен состоять не менее чем из 8 символов.

- В пароле могут присутствовать символы из числа следующих категорий:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) 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 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.

- 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.

3.4. Правила ввода пароля:

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

- Во время ввода пароля необходимо исключить возможность его под-сматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранение пароля:

- Запрещается хранить парольные карточки в общедоступных местах и осуществлять действия, которые могут скомпрометировать пароль.

- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие пароли, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

- своевременно сообщать Администратору ИСПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и Интернет

4.1. Работа в сетях общего доступа сети Интернет (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. 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 другие файлы.
- Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие).
- Запрещается нецелевое использование подключения к Сети.

С настоящей инструкцией ознакомлен:

_____ _____ «__» _____ 20__ г.

ФИО подпись

Приложение 5 к правилам работы с информационными системами Солигаличского муниципального округа Костромской области

Инструкция
по проведению антивирусного контроля на автоматизированном рабочем месте (АРМ)

1. Настоящая Инструкция предназначена для администратора безопасности и пользователей, обрабатывающих персональные данные с использованием средств автоматизации.

2. В целях обеспечения защиты автоматизированной информационной системы от программных закладок и программно-математического воздействия на обрабатываемые конфиденциальные данные на автоматизированных рабочих местах (АРМ) производится антивирусный контроль.

3. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности.

4. К установке и использованию в автоматизированной информационной системе и на АРМ разрешаются только лицензионные антивирусные средства, имеющие сертификат ФСТЭК.

5. На АРМ пользователя запрещается установка прикладного программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации на АРМ.

6. Пользователи АРМ при работе с информацией (ПО, БД, файлы) записанной на электронных носителях информации (Flash-карты, CD-диски, дискеты и т.п.) обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

7. Ярлык для запуска антивирусной программы должен быть вынесен на "Рабочий стол" операционной системы.

8. Обновление вирусных баз осуществляется ежедневно путём скачивания и установки антивирусных баз с сервера производителя антивирусного ПО.

Посредством настроек антивирусного средства и организации доступа к серверам разработчика антивирусного средства обновление можно выполнять в автоматическом режиме без участия пользователя АРМ. При невозможности настроить доступ АРМ к серверам

обновлений разработчика антивирусного средства Администратор информационной безопасности один раз в неделю производит установку пакетов.

9. При обнаружении компьютерного вируса в процессе эксплуатации АРМ либо сканирования съёмных электронных носителей информации пользователь обязан немедленно поставить об этом в известность администратора безопасности и прекратить какие-либо действия, связанные с обработкой конфиденциальной информации на АРМ.

10. По факту заражения АРМ компьютерным вирусом администратор безопасности производит «лечение» зараженных файлов путём выбора соответствующего пункта меню антивирусной программы, после чего вновь проводит антивирусный контроль файловой системы и обрабатываемых данных на АРМ. По результатам заражения АИС администратор безопасности проводит служебное расследование.

11. При обнаружении не поддающегося лечению вируса, администратор безопасности обязан удалить инфицированный файл в соответствующую папку антивирусного пакета, и проверить работоспособность АРМ. В случае отказа работоспособности АРМ - произвести восстановление и настройки соответствующего операционного и прикладного программного обеспечения.

12. О всех фактах заражения АИС и АРМ вредоносным программным обеспечением администратор безопасности обязан проинформировать ответственного за организацию обработки персональных данных либо главу администрации.

Приложение 6 к правилам работы с информационными системами Солигаличского муниципального округа Костромской области

Инструкция
по резервному копированию информации и восстановлению работоспособности ИС

1. Общие положения

1.1. В целях предупреждения возможности неблагоприятных последствий и обеспечения защиты важной или критичной для обеспечения работоспособности автоматизированных информационных систем информации от её случайного либо умышленного уничтожения, модификации или хищения, а также обеспечения её сохранности необходимо создавать её резервные копии.

1.2. Настоящая Инструкция разработана в соответствии с требованиями Федеральных законов от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации» и от 27.07.2006 №152-ФЗ «О персональных данных», постановлений Правительства РФ от 15.09.2008 №687 «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и от 01.11.2012 №1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» и иных нормативных документов и определяет общие правила резервирования обрабатываемых данных, в том числе при обработке информации ограниченного распространения (обработка персональных данных и иной конфиденциальной информации).

1.3. При осуществлении резервирования (резервного копирования) данных пользователи в своей работе руководствуется настоящей Инструкцией, иными внутренними нормативными документами и требованиями законодательства в сфере защиты информации ограниченного доступа.

1.4. Резервирование данных проводится для обеспечения восстановления работоспособности автоматизированных информационных систем (АИС), вызванной сбоями в работе либо отказами аппаратного и программного обеспечения, чрезвычайными обстоятельствами, ошибками пользователей и (или) иными внешними воздействиями, ведущими к полной или частичной утрате информации.

1.5. Требования настоящей Инструкции, связанные с резервным копированием критичной информации обязательны для исполнения всеми сотрудниками (пользователями), обрабатывающими такую информацию.

1.6. Администратор безопасности администрации осуществляет плановый и периодический контроль действий пользователей по обеспечению резервного копирования критически важных для обеспечения работоспособности АИС данных (информация о серийных номерах лицензионного ПО, настройках и т.п.).

2. Термины и определения

Автоматизированная информационная система (АИС) - взаимосвязанная совокупность данных, оборудования, программных средств, персонала, реализующая информационную технологию выполнения установленных функций, предназначенных для сбора, обработки, распределения, хранения, выдачи (предоставления) информации (по ГОСТ 34.003).

Критичная информация - любая важная информация, а также системное и прикладное программное обеспечение, утрата которых может привести к перебоям либо отказу в работе автоматизированной информационной системы и затруднению (либо невозможности) исполнения служебных обязанностей.

Резервное копирование - сохранение текущего состояния информации (системы) без обязательного сохранения предыдущего.

Съемный носитель информации - носитель информации, предназначенный для автономного хранения информации вне зависимости от места записи и использования (НЖМД, CD-DVD-диск, Flash-накопитель и т.п).

Гарантированное хранение - хранение, обеспечивающее целостность информации, определяемую требованиями федерального законодательства и внутренними организационно-распорядительными документами администрации.

3. Информация, подлежащая резервированию

В целях скорейшего восстановления работоспособности автоматизированной ИС и исключения неблагоприятных последствий, вызванных отказами в её работе либо утратой критичной информации, в администрации определен перечень информационных ресурсов, системного и прикладного ПО, подлежащих резервному копированию (Приложение 1), в который включен:

3.1. Персональные данные работников организации, обрабатываемые с использованием средств автоматизации и прикладного программного обеспечения в бухгалтерии.

3.2. Инсталляции системного и прикладного ПО, используемого для защиты и обработки критичной информации, персональных данных и иной конфиденциальной информации.

4. Порядок резервирования данных

Организация обеспечения резервного копирования обрабатываемой критичной информации, в том числе персональных данных, возложена на руководителей структурных подразделений администрации муниципального округа, в которых она обрабатывается (одного из его сотрудников).

4.1. Обязательному резервному копированию и гарантированному хранению подлежит информация, указанная в Приложении 1.

4.2. В качестве носителей, на которые осуществляется резервное копирование информации, в зависимости от сохраняемых информационных ресурсов, используются:

- папки на сетевом диске администрации;

- накопители на жестких магнитных носителях АРМ пользователей, физически разнесенные с накопителями, где происходит обработка критичной информации; - перезаписываемые или не перезаписываемые диски (CD, DVD, Blu-Ray).

4.3. К носителям, на которые производится резервное копирование, предъявляются следующие требования:

4.4.1. Наличие достаточного объема свободного дискового пространства либо свободной памяти для обеспечения надежного хранения резервных копий;

4.4.2. Носитель должен периодически проходить полную проверку целостности (не реже одного раза в 6 месяцев);

4.4.3. Носитель должен быть учтён по Журналу учёта электронных носителей с указанием наименования, информационной емкости, ответственного за его эксплуатацию сотрудника;

4.4.4. К носителю должен быть ограничен физический доступ посторонних лиц, в том числе по сети. Его хранение осуществляется в местах с ограниченным доступом (запираемый шкаф, сейф и т.п.);

4.4.5. Ход выполнения установленных требований соблюдения установленных правил хранения и доступа, целостности ячеек памяти и работоспособности осуществляется на регулярной основе в соответствии с планом проведения внутренних проверок.

4.5. Период сохранения резервных копий определяется исходя из целесообразности обеспечения гарантированного сохранения тех или иных информационных ресурсов (частота внесения изменений в данные, критичность их утраты и т.п.) и производится по окончании рабочего времени ежеквартально, ежегодно с сохранением информации за указанный период + 1 день.

5. Учёт материальных носителей резервных копий

5.1. В целях обеспечения сохранности резервируемой в администрации ведётся журнальный учёт электронных носителей, на которых сохраняются резервные копии критичной информации. Журнал учёта электронных носителей информации (Приложение 2) ведётся ответственным за организацию работы с персональными данными.

5.2. Сотрудник структурного подразделения администрации, отвечающий за резервное копирование критичной информации, обязан зарегистрировать электронный носитель по Журналу учёта и в дальнейшем хранить его в недоступном для посторонних лиц месте (запираемом шкафу, сейфе или иных защищенных местах хранения).

5.3. Уничтожение электронных носителей с резервными копиями (при необходимости) производится членами экспертной комиссии администрации на основании принятого ими решения в соответствии с установленным порядком.

6. Порядок восстановления работоспособности ИС

6.1. В случае потери (уничтожения, модификации) критичной информации пользователь информационных ресурсов ИСПДн либо ответственный работник обязан сообщить руководителю структурного подразделения о факте происшедшего сбоя в работе информационной системы, в результате которого произошла утрата данных. При этом сотрудник сообщает о возможных признаках сопутствующих отказу в работе АИС и принимает незамедлительные меры по восстановлению утраченной информации в кратчайший срок.

6.2. При потере критичной информации хранящейся на сетевом диске локальной информационной системы восстановление производится при участии администратора безопасности администрации.

6.3. По итогам происшедшего инцидента с утратой критичной информации в целях предотвращения подобных фактов в дальнейшем администратором безопасности проводится разбирательство с выявлением причин инцидента и лиц, допустивших нарушение.

7. Ответственность за нарушение установленного порядка резервирования данных

7.1. Персональная ответственность за обеспечение безопасного хранения критичной информации пользователя в соответствии с установленным порядком возлагается на ответственных работников, обрабатывающих эту информацию.

7.2. Ответственность за обеспечение резервного копирования критичной информации, обрабатываемой и сохраняемой в ИСПДн, возлагается на руководителя и ответственных работников подразделений.

7.3. Хранение резервных копий и инсталляций эксплуатируемого ПО, серийных номеров и регистрационных кодов возлагается на администратора безопасности.

7.4. Нарушение требований настоящей Инструкции влечёт за собой дисциплинарную ответственность в соответствии с трудовым законодательством РФ.

7.5. К лицам, нарушившим установленный порядок резервирования критичной информации, обеспечения сохранности и уничтожения электронных носителей информации

ограниченного доступа, вследствие которых произошло нанесение материального ущерба организации, могут быть приняты меры по возмещению убытков и компенсации морального вреда[1].

[1] Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению установленного порядка резервирования или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

Приложение 1 к инструкции по резервному копированию информации и восстановлению работоспособности ИС

ПЕРЕЧЕНЬ
критичных информационных ресурсов, подлежащих резервному копированию

№ п/п	Наименование информационного ресурса	Подразделение (сотрудник) ответственное за резервирование	Период резервирования	Носитель
1.	1С: Предприятие, Зарплата и кадры	Проводится силами сторонней организации, ответственной за сопровождение информационного ресурса	При обновлении программного обеспечения и возникновении критических ошибок	Жесткий диск бухгалтера МКУ «Бюджетное отраслевое учреждение» Солигаличского муниципального округа Костромской области
2.	Системное ПО	Администратор безопасности	При установке	Съемный носитель или жесткий диск пользователя, файловый сервер
3.	Прикладное ПО	Администратор безопасности	При установке	Съемный носитель или жесткий диск пользователя, файловый сервер

Приложение 2 к инструкции по резервному копированию информации и восстановлению работоспособности ИС

Журнал учета съемных носителей информации
администрации Солигаличского муниципального округа Костромской области

п\п	Наименование носителя	Объем носителя	Учетный номер носителя	ФИО лица, получившего носитель в пользование, его подпись дата выдачи	Дата сдачи носителя, ФИО и подпись лица, осуществившего приемку	Сведения об уничтожении СНИ

п\п	Наименование носителя	Объем носителя	Учетный номер носителя	ФИО лица, получившего носитель в пользование, его подпись дата выдачи	Дата сдачи носителя, ФИО и подпись лица, осуществившего приемку	Сведения об уничтожении СНИ

Приложение 3 к инструкции по резервному копированию информации и восстановлению работоспособности ИС

АКТ
уничтожения съемных носителей информации
администрации Солигаличского муниципального округа Костромской области

Комиссия, наделенная полномочиями распоряжением администрации муниципального округа от_____ №___ в составе:

Председатель комиссии: _____(_____)

Члены комиссии: _____(_____)

_____(_____)

провела отбор съемных носителей конфиденциальной информации (персональных данных), не подлежащих дальнейшему хранению:

№ п.п.	Дата	Учетный номер носителя	Примечание
1			
2			

Всего съемных носителей_____(цифрами и прописью)

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

Перечисленные съемные носители уничтожены

_____

путем (разрезания, демонтажа и т.п.)

_____

Председатель комиссии:

_____ (___/_____/_____)

Члены комиссии:

_____(___/_____/_____)

_____(___/_____/_____)

_____(___/_____/_____)

Подпись Дата

Приложение 7 к правилам работы с информационными системами Солигаличского муниципального округа Костромской области

ЧАСТНАЯ МОДЕЛЬ
актуальных угроз безопасности информации
и вероятного нарушителя информационной системы персональных данных
администрации Солигаличского муниципального округа Костромской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

В соответствии со статьей 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", оператор персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Угрозы безопасности персональных данных при их обработке в информационной системе персональных данных (далее - ИСПДН) администрации Солигаличского муниципального округа Костромской области пользователей, так и со специально осуществляемыми неправомерными действиями третьих лиц (отдельных организаций и граждан), а также иными источниками угроз.

Угрозы безопасности персональных данных могут быть реализованы за счёт утечки персональных данных по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при её передаче по каналам связи, технические каналы утечки акустической (речевой) и видовой информации) либо за счёт несанкционированного доступа с использованием соответствующего программного обеспечения.

Разработка модели угроз проведена на основании исходных параметров ИСПДн, определяемых в соответствии с предложенной ФСТЭК России Методикой определения угроз безопасности персональных данных, с привлечением в качестве консультантов сотрудников, имеющих необходимую подготовку и практический опыт.

2. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Вредоносная программа (ВП) - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера, входящего в состав информационной системы персональных данных - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации - возможность получения информации и её использования.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран (МСЭ) - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль информации, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (НСД) (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие установленные правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

Побочные электромагнитные излучения и наводки (ПЭМИН) - электромагнитные излучения и наводки в виде электрических и магнитных полей от средств обработки защищаемой информации, присутствующих в физической среде.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных (УБПДн) - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость ИСПДн - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

3. РАЗРАБОТКА АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ

Определение исходной защищенности ИСПДн

В соответствии с "Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных", экспертным путём были определены характеристики исходной защищенности ИСПДн, которые сведены в таблицу 1 и имеют следующие значения:

Таблица 1

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению: - распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	-	-	-
- городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	-	-	-
- корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	-	-	-
- локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	-	-	-
- локальная ИСПДн, развернутая в пределах одного	-	+	-

здания.			
2. По наличию соединения с сетями общего пользования: - ИСПДн, имеющая многоточечный выход в сеть общего пользования;	-	-	-
- ИСПДн, имеющая одноточечный выходв сеть общего пользования;	-	+	-
- ИСПДн, физически отделенная от сети общего пользования.	-	-	-
3. По встроенным (легальным) операциям с записями баз персональных данных: - чтение, поиск;	-	-	-
- запись, удаление, сортировка;	+	-	-
- модификация, передача.	-	-	-
4. По разграничению доступа к персональным данным:			
- ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект персональных данных;	+	-	-
- ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	-	-	-
- ИСПДн с открытым доступом.	-	-	-
5. По наличию соединений с другими базами персональных данных иных ИСПДн: - интегрированная ИСПДн (организация использует несколько баз персональных данных ИСПДн, при этом организация не является владельцем всех используемых баз персональных данных);	+	-	-
- ИСПДН, в которой используется одна база персональных данных, принадлежащая организации - владельцу данной ИСПДн.	-	-	-
6. По уровню обобщения (обезличивания) персональных данных: - ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	-	-	-
- ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	-	-	-
- ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта персональных данных).	-	+	-
7. По объему персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: - ИСПДн, предоставляющая всю базу персональных данных;	-	-	-
- ИСПДн, предоставляющая часть персональных данных;	-	-	-
- ИСПДн, не предоставляющие никакой информации.	-	+	-
ИТОГО:	3	4	0
	42, 84%	57, 16%	0 %
Исходная степень защищенности имеет средний уровень	5		

Исходя из вышеизложенного:

С учетом полученных уровней защиты ИСПДн следует, что более 70% оценок имеют средний и высокий уровень исходной защищенности ИСПДн, что позволяет определить уровень исходной защищенности информационной системы персональных данных как "средний" с коэффициентом = 5.

По данным обследования ИСПДн администрации Солигаличского муниципального округа Костромской области определена как типовая модель угроз безопасности персональных данных, обрабатываемая в локальной информационной системе персональных данных, имеющая подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, доступ к ИСПДн осуществляется в соответствии с матрицей доступа сотрудников предприятия, был сформирован перечень возможных угроз (таблица 2).

При составлении перечня актуальных угроз безопасности персональных данных каждой градации вероятности возникновения угрозы ставился в соответствие числовой коэффициент, а именно:

для маловероятной угрозы - 0;

для низкой вероятности угрозы - 2;

для средней вероятности угрозы - 5;

для высокой вероятности угрозы - 10,

Наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о наличии возможности реализации данной угрозы, которая определена по формуле:

$$Y= (Y1+ Y2)/20$$

По значению коэффициента реализуемости угрозы Y была сформирована вербальная интерпретация реализуемости угрозы, которая отражается следующим образом:

если, то возможность реализации угрозы признается низкой;

если, то возможность реализации угрозы признается средней;

если, то возможность реализации угрозы признается высокой;

если, то возможность реализации угрозы признается очень высокой.

В соответствии с "Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" после определения коэффициентов реализуемости угрозы на основе мнения экспертов по каждой угрозе была определена опасность её реализации по трём значениям:

низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Данные показатели занесены в таблице 2.

С учётом совокупности всех показателей и оценок угроз безопасности ИСПДн, в соответствии с методикой ФСТЭК РФ, была осуществлена оценка актуальности возможных угроз, которая приведена в таблице 2.

Оценка актуальности угроз ИСПДн администрации Солигаличского муниципального округа Костромской области

Таблица 2

	Угрозы ИСПДн	Y2	Коэфф. реализуемости угрозы Y	Опасность реализуемой угрозы	Актуальность угрозы
	Угрозы утечки информации по техническим каналам				
	угрозы утечки акустической (речевой) информации	0	0,25	низкая опасность	неактуальна
	угрозы утечки визуальной информации	0	0,25	низкая	неактуаль

				опасность	на
	угрозы утечки информации по каналу ПЭМИН	0	0,25	низкая опасность	неактуальна
	Угрозы НСД к персональным данным				
	Угрозы непосредственного доступа				
	угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	0	0,25	средняя опасность	неактуальна
	угрозы, реализуемые после загрузки операционной системы и направленные на осуществление несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)	5	0,5	средняя опасность	актуальна
	угрозы внедрения вредоносных программ	5	0,5	средняя опасность	актуальна
	Угрозы удаленного доступа				
	угрозы "анализа сетевого трафика"с перехватом информации, передаваемой по локальной сети, а также во внешние сети и принимаемой из внешних сетей	0	0,25	средняя опасность	неактуальна
	угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.;	0	0,25	высокая опасность	неактуальна
	угрозы получения НСД путем подмены доверенного объекта;	0	0,25	низкая опасность	неактуальна
0	угрозы выявления паролей	0	0,25	средняя опасность	неактуальна
1	угрозы типа "отказ в обслуживании"	5	0,5	средняя опасность	актуальна
2	угрозы удалённого запуска приложений	0	0,25	низкая опасность	неактуальна
3	угрозы внедрения по сети вредоносных программ.	5	0,5	средняя опасность	актуальна
4	угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации;	5	0,5	средняя опасность	актуальна
5	угрозы сканирования, направленные на выявление типа ОС ИСПДн, сетевых адресов рабочих станций, открытых	5	0,5	высокая опасность	актуальна

	портов и служб, открытых соединений и др.;				

4. РАЗРАБОТКА МОДЕЛИ ВЕРОЯТНОГО НАРУШИТЕЛЯ

В целях определения оценки вероятности угроз безопасности конфиденциальной информации, в том числе персональных данных, в администрации Солигаличского муниципального округа в соответствии с Положением о методах и способах защиты информации в информационных системах персональных данных разработана модель нарушителя.

Нарушитель - физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации, в том числе персональных данных, при их обработке техническими средствами. С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПДн, нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена - внешние нарушители;

- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн - внутренние нарушители.

В соответствии с Базовой моделью угроз безопасности персональных данных при обработке их в информационных системах, угрозу для ИСПДн администрации Солигаличского муниципального округа могут представлять следующие типы предполагаемых нарушителей:

внешние нарушители:

- недобросовестные партнеры;

- внешние субъекты (физические лица).

внутренние нарушители:

- лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к персональным данным - сотрудники, действующие преднамеренно;

- зарегистрированные пользователи ИСПДн, имеющие санкционированный доступ к ресурсам персональных данных с рабочего места - сотрудники действующие непреднамеренно;

- зарегистрированные пользователи с полномочиями системного администратора ИСПДн;

- программисты - разработчики прикладного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте;

- лица, обеспечивающие эксплуатацию и ремонт технических средств на оборудовании ИСПДн.

На основании данных о предполагаемых вероятных нарушителях, параметров исходной защищенности ИСПДн и сформированных угроз безопасности был сформирован перечень действий, способствующий реализации угроз и определены методы и способы защиты персональных данных (таблица 3).

Таблица 3

	Действия, приводящие к реализации угроз персональным данным	Используемые меры защиты
	Внешние нарушители:	
	Осуществление несанкционированного доступа к линиям и каналам связи, выходящим за пределы служебных помещений;	Организационные меры, граница контролируемой зоны.
	Осуществление несанкционированного доступа через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;	Антивирусное ПО, Брандмауэр
	Осуществление несанкционированного доступа к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;	Антивирусное ПО
	Осуществление несанкционированного доступа через элементы информационной инфраструктуры ИСПДн, которые	Организационные меры

	в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны;	
	Получение доступа к фрагментам информации, содержащей персональные данные и передающейся по внутренним каналам связи ИСПДн;	Организационные меры
	Обладание фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;	Конфиденциальная информация
	Знание имен и выявление учётных данных (логин+пароль) зарегистрированных пользователей;	Организационная мера, периодическая смена пароля
	Знание по меньшей мере одно легального имени доступа;	Конфиденциальная информация
	Обладание всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных;	Организационная мера, конфиденциальная информация
	Может располагать конфиденциальными данными, к которым имеет доступ;	Организационные меры
	Может располагать информацией о топологии ИСПДн на базе локальной информационной системы, через которую он осуществляет доступ, и составе технических средств ИСПДн;	Организационные меры
	Возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.	Организационные меры
	Обладание полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн;	Конфиденциальная информация, ограничение круга лиц по доступу
0.	Обладание полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;	Конфиденциальная информация, ограничение круга лиц по доступу
1.	Получение доступа к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;	Конфиденциальная информация, ограничение круга лиц по доступу
2.	Получение доступа ко всем техническим средствам сегмента (фрагмента) ИСПДн;	Конфиденциальная информация, ограничение круга лиц по доступу
3.	Обладание правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.	Ограничение круга лиц по доступу
4.	Обладание полной информацией о системном и прикладном программном обеспечении ИСПДн;	Ограничение круга лиц по доступу
5.	Обладание полной информацией о технических средствах и конфигурации ИСПДн;	Ограничение круга лиц по доступу
6.	Получение доступа ко всем техническим средствам обработки информации и данным ИСПДн;	Ограничение круга лиц по доступу
7.	Обладание правами конфигурирования и административной настройки технических средств ИСПДн.	Ограничение круга лиц по доступу
	Обладание информацией об алгоритмах и программах	Организационные

8.	обработки информации на ИСПДн;	меры, конфиденциальная информация
9.	Обладание возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;	Исключено на стадии закупки оборудовани

5. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

При разработке системы защиты персональных данных необходимо учитывать следующие рекомендации, обеспечивающие нейтрализацию предполагаемых угроз и снижение вероятности утечки информации в соответствии с классом ИСПДн администрации Солигаличского муниципального округа Костромской области актуальными угрозами:

Подсистема управления доступом:

* идентификация и проверка подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю сроком действия 90 суток, длиной не менее восьми буквенно-цифровых символов.

Межсетевое экранирование:

* принятие решения по фильтрации для каждого сетевого пакета независимо;

* идентификация и аутентификация администратора МСЭ при его локальных запросах на доступ, возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия;

* регистрация входа (выхода) администратора МСЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

* контроль целостности своей программной и информационной части;

* восстановление после сбоев и отказов оборудования;

* при удалённых запросах блокирование доступа не идентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату информации;

* оперативное восстановление свойств экранирования.

Защита от угроз программно-математического воздействия (ПМВ):

* идентификация и аутентификация субъектов доступа при входе в ИСПДн;

* запрет на использование прав администратора на автоматизированных рабочих местах пользователей;

* запрет на загрузку ОС АРМ со съемных носителей информации.

Подсистема регистрации и учета:

* регистрация входа (выхода) субъекта доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и её программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

* учёт всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал учета съемных носителей;

* регистрация событий проверки и обнаружения ПМВ. В параметрах регистрации указываются время и дата проверки или обнаружения ПМВ, идентификатор субъекта доступа, инициировавшего данные действия, характер выполняемых действий по проверке, тип обнаруженной вредоносной программы (ВП), результат действий средства защиты по блокированию ПМВ;

* данные регистрации должны быть защищены от их уничтожения или модификации нарушителем;

* механизмы сохранения данных регистрации в случае сокращения отведенных под них ресурсов;

* механизмы просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров;

* автоматический непрерывный мониторинг событий, которые могут являться причиной реализации ПМВ (создание, редактирование, запись, компиляция объектов, которые могут содержать ВП);

* механизм анализа данных регистрации по шаблонам типовых проявлений ПМВ с автоматическим их блокированием и уведомлением ответственного за обработку и защиту персональных данных;

* проведение нескольких видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации.

Подсистема обеспечения целостности (при использовании средств защиты информации):

* целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ;

* средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности;

* проверка целостности модулей средства защиты от ПМВ, необходимых для корректного функционирования, при его загрузке с использованием контрольных сумм;

* возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности;

* механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм;

* физическая охрана ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации.

Подсистема антивирусной защиты:

* автоматическая проверка на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа;

* работоспособность механизмов автоматического блокирования обнаруженных ВП путём их удаления из программных модулей или уничтожения;

* регулярная (при первом запуске средств защиты персональных данных от ПМВ и с устанавливаемой периодичностью) проверка на предмет наличия в них ВП;

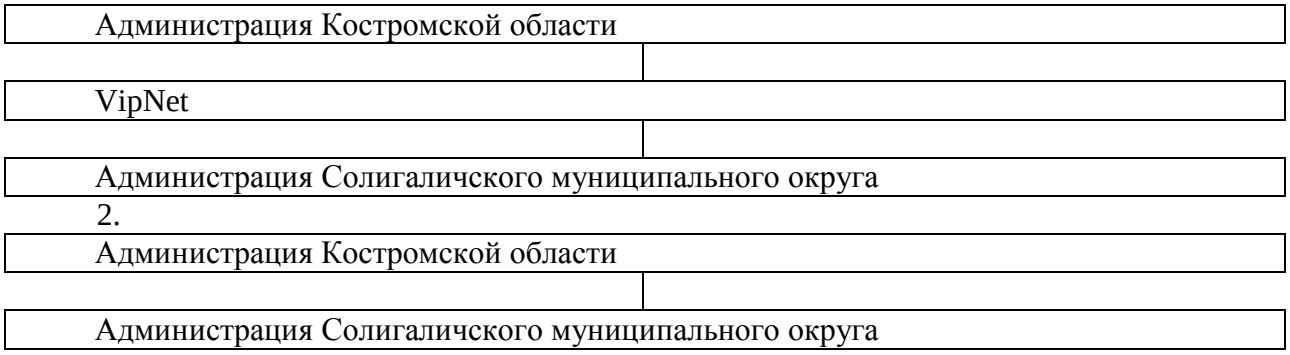
* автоматическая проверка ИСПДн на предмет наличия ВП при выявлении факта ПМВ;

* механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.

Приложение 8 к правилам работы с информационными системами Солигаличского муниципального округа Костромской области

СХЕМА ОРГАНИЗАЦИИ СЕТИ

1.



2.