РАСПОРЯЖЕНИЕ

АДМИНИСТРАЦИИ КРАСНОГВАРДЕЙСКОГО РАЙОНА
БЕЛГОРОДСКОЙ ОБЛАСТИ
ГОРОД БИРЮЧ

«19» августа 2011 г. № 906

Об утверждении Положения о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в органах местного самоуправления Красногвардейского района

В целях создания системы нормативно-правовых документов в сфере безопасности персональных данных, разрабатываемых в интересах формирования и развития системы защиты информации с ограниченным доступом в Красногвардейском районе, в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и во исполнение распоряжения Губернатора Белгородской области от 07 июля 2011 года № 459-рДСП «Об утверждении Положения о порядке организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных органов исполнительной власти, государственных органов области»:

1. Утвердить Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в органах местного самоуправления Красногвардейского района (далее – Положение, прилагается).

2. Рекомендовать главам администраций муниципальных образований района, руководителям структурных подразделений администрации района:

- обеспечить защиту персональных данных муниципальных служащих и работников органов местного самоуправления, замещающих должности, не являющиеся должностями муниципальной службы района, от неправомерного использования или утраты в порядке, установленном федеральными законами;

- назначить ответственных за обеспечение безопасности информации при использовании средств автоматизации, хранении и передаче персональных данных;

- издать соответствующие распорядительные документы в целях защиты персональных данных при их обработке в информационных системах.

3. Контроль за исполнением распоряжения возложить на заместителя главы администрации района – руководителя аппарата главы администрации района Бондаренко Л.В.

Глава администрации
Красногвардейского района **Н. Бровченко**

Утверждено
распоряжением администрации
Красногвардейского района

Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в органах местного самоуправления Красногвардейского района

1. Основные термины и определения

Персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор - муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных - действия (операции) с персональными данными, совершаемые работодателем в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или

других лиц.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Несанкционированный доступ (НСД) - получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

- доступ к информации или ее носителям с нарушением правил доступа к ним;

- ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Конфиденциальность персональных данных - обязательное для соблюдения работодателем или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Служебные сведения (служебная тайна) - служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

Уполномоченное оператором лицо - лицо, которому на основании договора оператор поручает обработку персональных данных.

Трансграничная передача персональных данных - передача персональных данных оператором через государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

2. Общие положения

2.1. Настоящее Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных органов местного самоуправления (далее - Положение) определяет порядок получения, хранения, передачи, автоматизированной обработки персональных данных в ИСПДн, а также без использования средств автоматизации в органах местного самоуправления.

2.2. Цель разработки настоящего Положения – определение порядка защиты ПДн от несанкционированного доступа и их разглашения.

2.3. Настоящее Положение разработано на основе и во исполнение:

- части 1 статьи 23, статьи 24 Конституции Российской Федерации,
- Кодекса Российской Федерации об административных правонарушениях;
- положений главы 14 Трудового кодекса Российской Федерации;
- Федерального закона от 27 июня 2006 года № 152-ФЗ «О персональных данных»;
- статей 28, 29, 30 Федерального закона от 02 марта 2007 года № 25-ФЗ «О муниципальной службе в Российской Федерации»;
- Указа Президента Российской Федерации от 06 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Указа Президента Российской Федерации от 30 мая 2005 года № 609 «Об утверждении положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;
- 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»;
- постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- приказа ФСТЭК от 05 февраля 2010 года № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

2.4. Положение определяет права и обязанности руководителей и муниципальных служащих, работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, порядок использования указанных данных в служебных целях, а также порядок взаимодействия по сбору, документированию, хранению и уничтожению ПДн.

3. Состав персональных данных

3.1. Документами, содержащими ПДн, являются:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учёт в налоговый орган и присвоения ИНН;
- документы воинского учёта;
- документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;
- личная карточка работника (форма Т-2);
- личный листок по учёту кадров;
- медицинское заключение о состоянии здоровья;
- документы, содержащие сведения о заработной плате, доплатах и надбавках;
- распоряжения о приеме лица на работу, об увольнении, а также о переводе на другую должность;
- другие документы, содержащие сведения составляющие ПДн.

3.2. Перечень ПДн, обрабатываемых в органах местного самоуправления района и под лежащих защите от несанкционированного доступа, согласовывается с кадровым подразделением и утверждается руководителем органа местного самоуправления района.

3.3. В целях информационного обеспечения могут создаваться общедоступные источники ПДн (в том числе справочники, адресные книги). В общедоступные источники ПДн с письменного согласия субъекта ПДн могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн, предоставленные субъектом ПДн.

Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

4. Основные условия безопасности при проведении обработки персональных данных

4.1. Обеспечение безопасности при проведении обработки ПДн в информационных системах ПДн органов местного самоуправления района с использованием средств автоматизации осуществляется в соответствии с требованиями 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», приказа ФСТЭК от 05 февраля 2010 года № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»,

нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

Оператор до начала обработки ПДн обязан уведомить уполномоченный Правительством Российской Федерации орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн.

Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов ПДн обработку ПДн:

1) относящихся к субъектам ПДн, которых связывают с оператором трудовые отношения;

2) полученных оператором в связи с заключением договора, стороной которого является субъект ПДн, если ПДн не распространяются, а также не предоставляются третьим лицам без согласия субъекта ПДн и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что ПДн не будут распространяться без согласия в письменной форме субъектов ПДн;

4) являющихся общедоступными ПДн;

5) включающих в себя только фамилии, имена и отчества субъектов ПДн;

6) необходимых в целях однократного пропуска субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в ИСПДн, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные ИСПДн, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов ПДн.

4.2. Обработка ПДн осуществляется:

- после получения согласия субъекта ПДн, составленного по форме со гласно приложению № 1 к настоящему Положению, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона от 27 июня 2006 года № 152-ФЗ «О персональных данных»;

- после направления уведомления об обработке ПДн, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27 июня 2006 года № 152-ФЗ «О персональных данных»;

- после принятия необходимых мер по защите ПДн.

4.3. В органах местного самоуправления решением руководителя назначается ответственный за обеспечение защиты ПДн и определяется перечень лиц, допущенных к обработке ПДн. Типовая форма регламента специалиста по обеспечению безопасности персональных данных приведена в приложении № 3.

4.4. Лица, допущенные к обработке ПДн, в обязательном порядке под роспись должны ознакомиться с настоящим Положением и подписать обязательство о неразглашении информации, содержащей ПДн, по форме согласно приложению № 2 к настоящему Положению.

4.5. Запрещается:

- обрабатывать ПДн в присутствии лиц, не допущенных к их обработке;
- осуществлять ввод ПДн под диктовку.

4.6. Не допускается обработка ПДн в ИСПДн с использованием средств автоматизации:

- при отсутствии установленных и настроенных сертифицированных средств защиты информации;
- при отсутствии утвержденных организационных документов о порядке эксплуатации ИСПДн.

5. Сбор, обработка и хранение персональных данных

5.1. Сбор ПДн муниципальных служащих и работников органов местного самоуправления, замещающих должности, не являющиеся должностями муниципальной службы района.

Документы, содержащие ПДн, создаются путем:

а) копирования оригиналов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и другие документы);

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

в) получения оригиналов необходимых документов (трудовая книжка, личный листок по учету кадров, медицинское заключение).

5.2. Обработка ПДн муниципальных служащих и работников органов местного самоуправления, замещающих должности, не являющиеся должностями муниципальной службы района, осуществляется исключительно в целях:

а) обеспечения соблюдения законов и иных нормативных правовых актов;

б) содействия в трудоустройстве;

в) обеспечения личной безопасности;

г) контроля количества и качества выполняемой работы;

д) обеспечения сохранности имущества.

5.3. ПДн следует получать лично у муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, за исключением случаев, если получение возможно только у

третьей стороны. Получение ПДн от третьих лиц возможно только при уведомлении муниципальных служащих и работников органов местного самоуправления, замещающих должности, не являющиеся должностями муниципальной службы района, об этом заранее и с их письменного согласия.

В уведомлении о получении ПДн у третьих лиц должна содержаться следующая информация:

а) цели получения ПДн;

б) предполагаемые источники и способы получения ПДн;

в) характер подлежащих получению ПДн;

г) последствия отказа муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, дать письменное согласие на их получение.

5.4. Органы местного самоуправления не имеют права получать и обрабатывать ПДн муниципальных служащих и работников органов местного самоуправления, замещающих должности, не являющиеся должностями муниципальной службы района, об их политических, религиозных иных убеждениях и частной жизни, равно как ПДн об их членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законодательством.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации органы местного самоуправления вправе получать и обрабатывать данные о частной жизни муниципальных служащих и работников органов местного самоуправления, замещающих должности, не являющиеся должностями муниципальной службы района, только с их письменного согласия.

5.5. При принятии решений, затрагивающих интересы муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, органы местного самоуправления района не имеют права основываться на ПДн, полученных исключительно в результате их автоматизированной обработки без согласия муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района.

5.6. К сведениям, содержащим ПДн, как на бумажных, так и на электронных носителях информации, доступ разрешен лицам, которые непосредственно используют ПДн муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, в служебных целях. Перечень должностных лиц в органах местного самоуправления района, использующих ПДн в служебных целях:

- начальник кадрового подразделения;

- специалист кадрового подразделения;

- руководитель отдела учета и отчетности – главный бухгалтер администрации района;

- специалисты отдела учета и отчетности.

Доступ к ПДн муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, без специального разрешения имеют:

- руководитель органа местного самоуправления района;

- заместители руководителя органа местного самоуправления района;

- начальники структурных подразделений администрации района - в отношении ПДн муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, находящихся в их непосредственной подчиненности в соответствии с их должностными регламентами (инструкциями).

Кроме перечня лиц, допущенных к ПДн, в органах местного самоуправления района разрабатывается разрешительная система доступа (матрица доступа) к информационным ресурсам, ИСПДн и связанным с ее использованием работам, документам. Полный перечень работ и разрабатываемых документов по обеспечению безопасности персональных данных при их обработке в ИСПДн оформляется согласно приложения к Протоколу заседания рабочей группы по информатизации, телекоммуникациям и защите информации в Белгородской области при Совете Губернатора области 21 мая 2010 года.

5.7. Хранение ПДн в органах местного самоуправления района:

а) ПДн, содержащиеся на бумажных носителях, хранятся в запираемых шкафах, сейфах, установленных на рабочих местах лиц, ответственных за обработку ПДн в органах местного самоуправления района;

б) ПДн в электронном виде хранятся на отдельных серверах, которые не имеют подключений к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), либо на жестких дисках автоматизированных рабочих мест, к которым имеют доступ только лица, ответственные за обработку ПДн в органах местного самоуправления района;

5.8. ПДн, содержащиеся на бумажных носителях, сдаются в архив.

6. Доступ к персональным данным

6.1. К ПДн муниципальных служащих и работников органов местного самоуправления района имеют доступ только те, кому ПДн необходимы в связи с исполнением ими трудовых обязанностей.

6.2. В целях выполнения порученного задания и на основании служеб ной записки с положительной резолюцией руководителя органа местного самоуправления района доступ к ПДн может быть предоставлен иному

муниципальному служащему или работнику органа местного самоуправления района, замещающему должность, не являющуюся должностью муниципальной службы района службы района, должность которого не включена в перечень должностных лиц органа местного самоуправления, уполномоченных на обработку ПДн и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих ПДн.

6.3. Уполномоченные лица имеют право получать только те ПДн, кото рые необходимы им для выполнения конкретных функций в соответствии с их должностным регламентом (инструкцией).

6.4. Муниципальные служащие и работники органа местного самоуправления района, замещающие должности, не являющиеся должностями муниципальной службы района, имеют право на свободный доступ к своим ПДн, включая право на получение копии любой записи (за исключением случаев предусмотренных федеральным законодательством), содержащей их ПДн.

6.5. Муниципальные служащие и работники органа местного самоуправления района, замещающие должности, не являющиеся должностями муниципальной службы района, имеют право вносить изменения в свои данные в случае обнаружения в них неточностей.

6.6. Муниципальные служащие и работники органа местного самоуправления района, замещающие должности, не являющиеся должностями муниципальной службы района, имеющие доступ к ПДн в органе местного самоуправления в связи с исполнением трудовых обязанностей, обеспечивают хранение информации, содержащей ПДн, исключающее доступ к ним третьих лиц.

6.7. В период отпуска, служебной командировки и иных случаях дли тельного отсутствия на рабочем месте муниципального слу жащего или работника органов местного самоуправления района, замещающего должность, не являющуюся должностью муниципальной службы района, он обязан передать документы и иные носители, содержащие ПДн лицу, на которое приказом руководителя органа местного самоуправления будет возложено исполнение его трудовых обязанностей.

6.8. В случае если такое лицо не назначено, то документы и иные носители, содержащие ПДн, передаются другому муниципальному слу-жащему или работнику органов власти области, замещающего должность, не являющуюся должностью муниципальной службы района, имеющему доступ к ПДн, по указанию руководителя структурного подразделения.

При увольнении муниципального служащего или работника органа местного самоуправления района, замещающего должность, не являющуюся должностью муниципальной службы района, имеющего доступ к ПДн, документы и иные носители, содержащие ПДн, передаются другому муниципальному служащему или работнику органа местного самоуправления района, замещающему должность, не являющуюся

должностью муниципальной службы района, имеющему доступ к ПДн, по указанию руководителя структурного подразделения.

6.7. Процедура оформления доступа к ПДн уполномоченного муниципального служащего или работника органа местного самоуправления района, замещающего должность, не являющуюся должностью муниципальной службы района, включает в себя:

- ознакомление под роспись с настоящим Положением, иными нормативными актами (приказами, распоряжениями, инструкциями и т.п.), регулирующими обработку и защиту ПДн в органах местного самоуправления района;

- истребование письменного обязательства о соблюдении конфиденциальности ПДн и соблюдении правил их обработки, подготовленного по установленной форме (приложение № 2).

6.8. Кадровое подразделение органа местного самоуправления вправе передавать ПДн муниципальных служащих и работников органа местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, в бухгалтерию и иные структурные подразделения органа местного самоуправления района, в случае если эти данные необходимы для исполнения уполномоченными муниципальными служащими или работниками органов местного самоуправления района, замещающими должности, не являющиеся должностями муниципальной службы района соответствующих структурных подразделений своих трудовых обязанностей.

При передаче ПДн муниципальные служащие и работники органа местного самоуправления района, замещающие должности, не являющиеся должностями муниципальной службы района, кадрового подразделения предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и истребуют от этих лиц письменное обязательство в соответствии с пунктом 4.4. настоящего Положения.

6.9. Передача (обмен и т.д.) ПДн между подразделениями органа местного самоуправления района осуществляется только между муниципальными служащими, работниками органов местного самоуправления района, замещающими должности, не являющиеся должностями муниципальной службы района, которые имеют доступ к ПДн в рамках исполнения своих должностных регламентов и инструкций.

6.10. Передача ПДн муниципальных служащих и работников органа местного самоуправления, замещающих должности, не являющиеся должностями муниципальной службы района, третьим лицам осуществляется только с их письменного согласия, которое оформляется по установленной форме и должно включать в себя:

- фамилию, имя, отчество, должность;

- наименование и юридический адрес органа местного самоуправления района, получающего согласие;

- цель передачи ПДн;

- перечень ПДн, на передачу которых дается согласие;

- срок, в течение которого действует согласие, а также порядок его отзыва.

Согласие муниципальных служащих и работников органа местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, на передачу их ПДн третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью; когда третьи лица оказывают услуги органу местного самоуправления на основании заключенных договоров, а также в случаях, установленных Федеральным законом от 27 июня 2006 года № 152-ФЗ «О персональных данных» и настоящим Положением.

6.11. Не допускается передача ПДн муниципальных служащих и работников органа местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, в коммерческих целях без их письменного согласия.

6.12. Муниципальные служащие и работники органа местного самоуправления района, замещающие должности, не являющиеся должностями муниципальной службы района, передающие ПДн третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих ПДн. Акт должен содержать следующие условия:

- уведомление лица, получающего данные документы, об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена;

- предупреждение об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральным законодательством.

Передача документов (иных материальных носителей), содержащих ПДн, осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг органу местного самоуправления района;

- соглашения о неразглашении конфиденциальной информации либо наличия в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту ПДн;

- письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, со держащей ПДн, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

Ответственность за соблюдение вышеуказанного порядка предоставления ПДн муниципальных служащих и работников органа местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, несет ответственное лицо, а также руководитель структурного подразделения, осуществляющего передачу ПДн третьим лицам.

6.13. Представителю (в том числе адвокату) муниципального служащего и работника органа местного самоуправления района, замещающего должность, не являющуюся должностью муниципальной службы района, ПДн передаются в порядке, установленном действующим законодательством и настоящим Положением.

Информация передается при наличии одного из документов:

- нотариально заверенной доверенности представителя;

- письменного заявления муниципального служащего, либо работника органа местного самоуправления района, замещающего должность, не являющуюся должностью муниципальной службы района написанного в присутствии ответственного лица, допущенного к обработке ПДн органа местного самоуправления района (если заявление написано не в присутствии ответственного лица, допущенного к обработке ПДн органа местного самоуправления района, то оно должно быть нотариально заверено).

Доверенности и заявления хранятся в отделе органа местного самоуправления района, где обрабатываются запрашиваемые ПДн муниципальных служащих или работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района.

6.14. Предоставление ПДн государственным органам, органам местного самоуправления производится в соответствии с требованиями действующего законодательства и настоящим Положением.

ПДн могут быть предоставлены родственникам или членам семьи муниципального служащего или работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, только с их письменного разрешения, за исключением случаев, когда передача ПДн без согласия допускается действующим законодательством Российской Федерации.

6.15. Доступ к электронным базам данных, содержащим ПДн муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, обеспечиваются системой паролей. Пароли устанавливаются начальниками или лицом, назначенным ответственным за обеспечение безопасности ПДн в структурных подразделениях органа местного самоуправления района, и сообщаются индивидуально муниципальным служащим или работникам органа местного самоуправления, замещающим должности, не являющиеся должностями муниципальной службы района, имеющим доступ к ПДн.

6.16. Запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами инфор мационной системы в электронном журнале обращений. Содержание элек тронного журнала обращений проверяется не реже 1 раза в месяц соответст

вующими должностными лицами или ответственным, который назначается руководителем органа местного самоуправления.

6.17. Статьей 12 Федерального закона от 27 июня 2006 года № 152-ФЗ «О персональных данных» предусмотрена трансграничная передача ПДн, которая может осуществляться на территории иностранных государств в сле дующих случаях:

- наличия согласия в письменной форме субъекта персональных данных;
- предусмотренных международными договорами Российской Феде рации по вопросам выдачи виз, международными договорами Российской Федерации об оказании правовой помощи по гражданским, семейным и уголовным делам, а также международным договорам Российской Федерации о реадмиссии;
- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения, обороны страны и безопасности государства;
- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

7. Защита персональных данных в органах местного самоуправления района

7.1. Защита ПДн муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, от неправомерного их использования или утраты обеспечивается органами местного самоуправления района в порядке, установлен ном федеральным законодательством.

7.2. Общую организацию защиты ПДн муниципальных слу жащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, осуществляет руководитель органа местного самоуправления района.

7.3. Начальник отдела кадров и/или лицо, назначенное ответственным за обеспечение безопасности информации в отделе кадров, организует:

- ознакомление с настоящим Положением под роспись муниципальных служащих и работников органа местного самоуправления, замещающего должности, не являющиеся должностями муниципальной службы района;
- в случае вступления иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся

должностями муниципальной службы района, также производится ознакомление под роспись;

- истребование с муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, письменного обязательства о соблюдении конфиденциальности ПДн в органах местного самоуправления района и соблюдении правил их обработки;

- общий контроль за соблюдением муниципальными служащими и работниками органа местного самоуправления района, замещающими должности, не являющиеся должностями муниципальной службы района мер по защите ПДн.

7.4. Организацию и контроль за защитой ПДн осуществляют непосредственно руководители муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, которые имеют доступ к ПДн.

Методическое руководство по защите ПДн осуществляет лицо, ответственное за обеспечение безопасности информации.

7.5. В целях обеспечения защиты сведений, хранящихся в электронных базах данных органов местного самоуправления района, от НСД, искажения и уничтожения информации, а также от иных неправомерных действий применяются следующие основные методы и способы защиты информации:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (матрица доступа), информационной системе и связанным с ее использованием работам, документам;

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, постоянная проверка элементов системы на наличие следов взлома;

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

- учет и хранение съемных носителей информации, их обращение, исключающее хищение, подмену и уничтожение;

- резервирование технических средств, дублирование массивов и носителей информации, учет всех защищаемых носителей информации с по мощью их маркировки и занесение учетных данных в журнал учета съемных носителей информации;

- использование средств защиты информации, прошедших процедуру оценки соответствия;

- использование защищенных каналов связи;

- размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку ПДн;

- контроль доступа в помещения информационной системы посторонних лиц;

- предотвращение внедрения в информационные системы вредонос ных программ (программ-вирусов) и программных закладок.

7.6. При взаимодействии ИСПДн с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с методами и способами, указанными в пункте 7.5. настоящего Положения, применяются следующие меры и способы защиты информации от НСД:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

- защита информации при ее передаче по каналам связи;

- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей; использование средств антивирусной защиты;

- централизованное управление системой защиты персональных данных информационной системы.

7.7. С целью получения общедоступной информации кроме методов и способов, указанных в пунктах 7.5, 7.6 настоящего Положения, применяются следующие методы и способы защиты информации:

- фильтрация входящих (исходящих) сетевых пакетов по правилам, заданным оператором (уполномоченным лицом);

- периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на информационные системы;

- активный аудит безопасности информационной системы на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

- анализ принимаемой по информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов.

7.8. При удаленном доступе к информационной системе через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) кроме методов и способов, указан-

ных в пунктах 7.5, 7.6 настоящего Положения, применяются следующие методы и способы защиты информации:

- проверка подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) данных;

- управление доступом к защищаемым персональным данным информационной сети;

- использование атрибутов безопасности.

7.9. При межсетевом взаимодействии отдельных информационных систем через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) кроме методов и способов, указанных в пунктах 7.5, 7.6. настоящего Положения, применяются следующие методы и способы защиты информации:

- создание защищенного канала связи, обеспечивающего защиту передаваемой информации;

- осуществление аутентификации взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных (использование цифровой электронной подписи и шифрования информации).

7.10. При межсетевом взаимодействии отдельных информационных систем разных операторов через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) кроме методов и способов, указанных в пунктах 7.5, 7.6 настоящего Положения, применяются следующие методы и способы защиты информации:

- создание защищенного канала связи, обеспечивающего защиту передаваемой информации;

- аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных;

- обеспечение предотвращения возможности отрицания пользователем факта отправки персональных данных другому пользователю;

- обеспечение предотвращения возможности отрицания пользователем факта получения персональных данных от другого пользователя.

7.11. Для исключения утечки персональных данных за счет побочных электромагнитных излучений и наводок в ИСПДн применяются следующие методы и способы защиты информации:

- использование технических средств в защищенном исполнении;

- использование средств защиты информации, прошедших в установлен ном порядке процедуру оценки соответствия;

- размещение объектов защиты в соответствии с предписанием на эксплуатацию;

- размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;

- обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

7.12. Если имеется функция воспроизведения информации акустическими средствами в ИСПДн, то используются методы и способы защиты акустической (речевой) информации. Методы и способы защиты акустической (речевой) информации заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена ИСПДн, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при воспроизведении информации акустическими средствами. Величина звукоизоляции определяется оператором исходя из характеристик помещения, его расположения и особенностей обработки ПДн в информационной системе.

7.13. Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

7.14. Для зашиты персональных данных в ИСПДн и выполнения пунктов 7.5 - 7.13 настоящего Положения органами местного самоуправления района привлекаются для выполнения специальных, аналитических и экспертных работ по защите информации специализированные организации-лицензиаты ФСТЭК и ФСБ России.

Специализированные организации, привлекаемые органами власти для оказания услуг по защите ПДн, должны иметь лицензии ФСТЭК и (или) ФСБ России на деятельность по защите информации (проведение контроля отсутствия недекларированных возможностей, аттестации технических средств, установки необходимых средств зашиты информации).

7.15. При обработке ПДн в информационной системе пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов), носителей информации, встроенных в технические средства, или съемных маркированных носителей;

б) недопущение физического воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

7.16. При обработке ПДн в информационной системе руководителем органа местного самоуправления района и лицами, ответственными за обеспечение безопасности в структурных подразделениях органов местного самоуправления района должны обеспечиваться:

а) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

б) учет лиц, допущенных к работе с ПДн в информационной системе, прав и паролей доступа;

в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

д) описание системы защиты ПДн.

7.17. Каждый съемный носитель, с записанными на нем ПДн, должен иметь маркировку, на которой указывается его уникальный учетный номер. Учет и выдачу съемных носителей ПДн осуществляют ответственные за обеспечение безопасности ПДн или делопроизводитель конфиденциальной информации в органах местного самоуправления района в журнале учета.

7.18. В случае выхода из строя техники, на которой проводилась обработка ПДн, вынос за пределы территории органов власти области с целью ремонта, замены и т.п. без согласования с руководителем или ответственным за обеспечение безопасности ПДн в подразделении органа местного самоуправления запрещается.

7.19. Съемные носители ПДн, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией, утвержденной распоряжением руководителя в органа местного самоуправления района. По результатам уничтожения носителей составляется акт, при необходимости уничтожения информации с носителей ПДн также составляется акт.

8. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

8.1. Права, обязанности, действия муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, в трудовые обязанности которых входит обработка ПДн муниципальных служащих и работников органов местного самоуправления района, замещающих должности, не являющиеся должностями муниципальной службы района, определяются их должностными регламентами (инструкциями).

8.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут ответственность в порядке, установленном действующим законодательством.

Начальник отдела муниципальной службы,
кадров и аналитической работы
администрации района **А. Криушин**

Приложение № 1
к Положению о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в органах местного самоуправления Красногвардейского района

Согласие на обработку персональных данных

Я, _____
(фамилия, имя, отчество)

_____

даю согласие _____
(наименование органа местного самоуправления)

_____,

адрес места нахождения:_____

_____

на обработку и использование данных, содержащихся в настоящем заявлении, с целью соблюдения действующего законодательства. Документ, удостоверяющий личность, _____
(наименование, номер и серия документа, кем и когда ыдан)

_____,

Адрес регистрации по месту жительства _____
(почтовый адрес)

_____

Адрес фактического проживания _____
(фактический адрес, контактный телефон)

_____

Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных и членов его семьи:

Фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы.

Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных:

обработка персональных данных будет осуществляться путем смешанной обработки, с передачей по внутренней сети юридического лица и без передачи по сети Интернет.

Я согласен на передачу своих персональных данных в целях обязательно социального страхования, обязательного медицинского страхования, похождения диспансеризации и других действий в соответствии с федешьным законодательством, содействия муниципальному служащему в прохождении муниципальной службы, в обучении и должностном росте, обеспечения личной безопасности муниципального служащего и членов его семьи, а также учета результатов исполнения им должностных обязанностей.

Я проинформирован, что под обработкой персональных данных понимаются действия (операции) с персональными данными в соответствии с пунктом 3 статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

В случае неправомерного использования предоставленных данных согласие отзывается письменным заявлением субъекта персональных данных.

Об ответственности за достоверность представленных сведений предупрежден(на).

Срок действия согласия - прекращение деятельности органа местного самоуправления (ликвидация или реорганизация).

«____» _____ 20 __ года Подпись _____ /_____/

Приложение № 2
к Положению о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в органах местного самоуправления Красногвардейского района

ОБЯЗАТЕЛЬСТВО

о неразглашении информации, содержащей персональные данные

Я,_____,
(Ф И.О муниципального служащего органа местного самоуправления)
исполняющий (ая) должностные обязанности по замещаемой должности ____
_____
(должность, наименование структурного подразделения)
предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, со держащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. В течение года после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к ответственности в соответствии с законодательством Российской Федерации.

_____ _____
(фамилия, инициалы) (подпись)

«____» _____ 20 ___ г.

Приложение № 3
к Положению о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в органах местного самоуправления Красногвардейского района

Регламент специалиста по обеспечению безопасности персональных данных

I. Общие положения

1.1. Настоящий должностной регламент специалиста по обеспечению безопасности персональных данных (далее - Регламент) определяет основные цели, функции и права специалиста по обеспечению безопасности персональных данных (далее - Специалист) в органах местного самоуправлении Красногвардейского района.

1.2. Специалист назначается распоряжением (или иным документом) руководителя органа местного самоуправления Красногвардейского района на основании Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного постановлением Совета Министров - Правительства Российской Федерации от 15 сентября 1993 года № 912-51, во исполнение Федерального закона «О персональных данных» 152-ФЗ от 27 июля 2006 года.

1.3. Специалист проводит свою работу согласно нормативным методическим документам Федеральной службы по техническому и экспортному контролю Российской Федерации, Федеральной службы безопасности Российской Федерации и иных уполномоченных законодательством органов в области обеспечения безопасности персональных данных.

1.4. Непосредственное руководство работой специалиста осуществляет заместитель руководителя органа местного самоуправления Красногвардейского района, курирующий вопросы защиты информации.

Назначение и освобождение от должности специалиста производится руководителем органа местного самоуправления.

1.5. Специалист назначается из числа муниципальных служащих либо работников органа местного самоуправления, замещающих должности, не являющиеся должностями муниципальной гражданской службы района, имеющих опыт работы по основной деятельности органа местного самоуправления района или в области защиты информации.

1.6. Специалисту выплачивается заработная плата, устанавливаются льготы и премирование в соответствии со штатным расписанием органа местного самоуправления.

1.7. Работа специалиста проводится в соответствии с планами работ, утверждаемыми непосредственным руководителем или руководителем органа местного самоуправления.

1.8. В своей работе специалист руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных, приказами и распоряжениями руководителя органа власти и другими руководящими документами по обеспечению безопасности персональных данных.

П. Основные функции специалиста

2.1. Проведение единой технической политики, организация и координация работ по обеспечению безопасности персональных данных в органе местного самоуправления Красногвардейского района.

2.2. Проведение мероприятий по организации обеспечения безопасности персональных данных, включая классификацию информационных систем персональных данных.

2.3. Проведение мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в том числе:

- мероприятий по размещению, охране, организации режима допуска в помещения, где ведется обработка персональных данных;
- мероприятий по закрытию технических каналов утечки персональных данных при их обработке;
- мероприятий по защите от несанкционированного доступа к персональным данным;
- мероприятий по выбору средств защиты персональных данных при их обработке.

2.4. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передачи их лицам, не имеющим права доступа к такой информации.

2.5. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

2.6. Недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование.

2.7. Обеспечение возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступак ним.

2.8. Постоянный контроль за обеспечением уровня защищенности персональных данных.

2.9. Участие в подготовке к аттестации по выполнению требований обеспечения безопасности персональных данных объектов информатизации, на которых обрабатываются персональные данные.

2.10. Разработка организационно-распорядительных документов по обеспечению безопасности персональных данных.

2.11. Организация расследования причин и условий появления нарушений безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.

2.12. Разработка предложений, участие в проводимых работах по совершенствованию системы безопасности персональных данных в органе власти области.

2.13. Проведение периодического контроля эффективности мер защиты персональных данных в органе власти области. Учет и анализ результатов контроля.

2.14. Подготовка отчетов о состоянии работ по обеспечения безопасности персональных данных в органе местного самоуправления.

III. Права специалиста

Специалист имеет право:

3.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных данных.

3.2. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.

3.3. Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.

3.4. Контролировать деятельность структурных подразделений органа местного самоуправления района в части выполнения ими требований по обеспечению безопасности персональных данных.

3.5. Вносить предложения руководителю органа местного самоуправления района приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.

3.6. Привлекать на договорной основе необходимых специалистов организаций-лицензиатов ФСТЭК для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

IV. Ответственность специалиста

4.1. Специалист несет персональную ответственность за:

- правильность и объективность принимаемых решений;

- правильное и своевременное выполнение приказов, распоряжений, указаний руководителя органа местного самоуправления по вопросам, входящим в возложенные на него функции;

- выполнение возложенных на него обязанностей, предусмотренных на стоящим Регламентом;

- соблюдение трудовой дисциплины, охраны труда;

- качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями.

- согласно действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.