АДМИНИСТРАЦИЯ ГОРОДА БЕЛГОРОДА

РАСПОРЯЖЕНИЕ

«28» мая 2015 г. № 575

Об утверждении Положения о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации города Белгорода

В соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», в целях создания системы организационно-распорядительных и нормативных документов в сфере безопасности персональных данных, разрабатываемых для формирования и развития системы защиты информации с ограниченным доступом:

1. Утвердить Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации города Белгорода.

2. Руководителям отраслевых (функциональных), территориальных органов и структурных подразделений администрации города руководствоваться в работе утвержденным положением.

3. Настоящее распоряжение подлежит размещению на официальном сайте органов местного самоуправления города Белгорода.

4. Контроль за исполнением распоряжения возложить на заместителя главы администрации города по внутренней и кадровой политике Медведеву О.И.

Глава администрации города Белгорода **С.Боженов**

Администрация города Белгорода Белгородской области РФ Отдел служебного документооборота

УТВЕРЖДЕНО
распоряжением администрации
города Белгорода
от «18» мая 2015 года № 575

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации города Белгорода

1. Общие положения

1.1. Настоящее Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации города Белгорода (далее - положение) определяет порядок получения, хранения, передачи, автоматизированной обработки персональных данных в информационных системах персональных данных (далее - ИСПДн), а также без использования средств автоматизации в администрации города Белгорода (далее - администрация), в том числе в структурных подразделениях администрации города Белгорода с правами юридического лица (далее - подразделения).

1.2. Цель разработки настоящего положения – определение порядка защиты персональных данных (далее - ПДн) от несанкционированного доступа (далее - НСД) и их разглашения.

1.3. Настоящее Положение разработано на основе и во исполнение:

- Конституции Российской Федерации;
- Трудового кодекса Российской Федерации;
- Федерального закона от 27 июня 2006 г. № 152-ФЗ «О персональных данных»;
- Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;
- Указа Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Федерального закона от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации».

1.4. Положение определяет права и обязанности руководителей и работников администрации и подразделений, при осуществлении обработки ПДн, порядок использования ПДн в служебных целях, а также порядок взаимодействия по сбору, документированию, хранению и уничтожению ПДн.

2. Состав персональных данных

2.1. Документами, содержащими ПДн, являются:
- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка;
- страховое свидетельство обязательного пенсионного страхования;
- свидетельство о постановке на учёт в налоговом органе;
- документы воинского учёта;
- документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;
- личная карточка работника;
- личный листок по учёту кадров;
- медицинское заключение о состоянии здоровья;
- документы, содержащие сведения о заработной плате, доплатах и надбавках;
- распорядительные документы о приеме лица на работу, об увольнении, а также о переводе на другую должность;
- другие документы, содержащие сведения составляющие ПДн.

2.2. В администрации и подразделениях составляется перечень обрабатываемых ПДн, подлежащих защите от НСД, и утверждается их руководителями.

2.3. 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.

3. Основные условия безопасности при проведении обработки персональных данных

3.1. Руководитель администрации, подразделения назначает ответственного за организацию обработки ПДн, подлежащих защите, из числа работников, и утверждает локальным актом.

До начала обработки ПДн администрация и подразделения обязаны уведомить уполномоченный Правительством Российской Федерации орган

по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных». Заполнение уведомления организует лицо, ответственное за организацию обработки ПДн. Уведомление заполняется на официальном сайте уполномоченного Правительством Российской Федерации органа по защите прав субъектов ПДн (Роскомнадзор).

Администрация и подразделения вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов ПДн обработку ПДн:

- обрабатываемых в соответствии с трудовым законодательством;

- полученных 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 исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн;

- 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 или раскрываться третьим лицам без согласия в письменной форме субъектов ПДн;

- сделанных субъектом ПДн общедоступными;

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

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

- 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;

- 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.

3.2. Администрацией и подразделениями обработка ПДн осуществляется:

- после получения согласия субъекта ПДн;

- после направления уведомления в уполномоченный Правительством Российской Федерации орган по защите прав субъектов ПДн об обработке ПДн, за исключением случаев, предусмотренных Федеральным законом от 27 июня 2006 г. № 152-ФЗ «О персональных данных»;

- после принятия необходимых мер по защите ПДн.

3.3. Непосредственное руководство работой ответственного за организацию обработки ПДн осуществляет руководитель администрации, подразделения.

Координацию работ лиц, ответственных за организацию обработки ПДн в администрации, подразделениях, осуществляет отдел информационных технологий и эксплуатации информационных систем управления делами аппарата администрации города Белгорода.

В своей работе ответственные за организацию обработки ПДн руководствуются законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных, приказами, распоряжениями и другими руководящими документами по обеспечению безопасности персональных данных.

Основными функциями ответственных лиц в администрации, подразделениях за организацию обработки ПДн являются:

- осуществление внутреннего контроля за соблюдением работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

- доведение до сведения работников положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

- организация приема и обработки обращений и запросов субъектов ПДн (и) или осуществление контроля за приемом и обработкой таких обращений и запросов.

Ответственные за организацию обработки ПДн несут персональную ответственность за:

- правильность и объективность принимаемых решений;

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

- соблюдение трудовой дисциплины, охраны труда;

- качество проводимых работ по обеспечению безопасности ПДн в соответствии с функциональными обязанностями;

- разглашение сведений ограниченного распространения, ставших известными по роду работы.

3.4. В администрации, подразделениях, локальным актом руководителя определяется перечень должностей служащих, уполномоченных на обработку ПДн.

Кроме перечня должностей служащих, уполномоченных на обработку ПДн, в администрации и подразделениях разрабатывается разрешительная система доступа (далее - матрица доступа) к информационным ресурсам, ИСПДн и связанным с ее использованием работам, документам. Матрица доступа утверждается руководителем структурного подразделения.

3.5. Запрещается:

- обрабатывать ПДн в присутствии лиц, не допущенных к их обработке;

- осуществлять ввод ПДн под диктовку.

3.6. 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.

4. Сбор, обработка и хранение персональных данных

4.1. Сбор ПДн субъектов ПДн в администрации и подразделениях.

Документы, содержащие ПДн, создаются путем:

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

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

- получения оригиналов необходимых документов (трудовая книжка, личный листок по учету кадров, медицинское заключение, и другие документы).

4.2. Обработка ПДн работников администрации и подразделений осуществляется исключительно в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;

- содействия в трудоустройстве;

- обеспечения личной безопасности;

- контроля количества и качества выполняемой работы;

- обеспечения сохранности имущества.

4.3. ПДн следует получать лично у работников, за исключением случаев, если получение возможно только у третьей стороны. Получение ПДн от третьих лиц возможно только при уведомлении работников, об этом заранее и с их письменного согласия.

4.4. Администрация и подразделения не имеют права получать и обрабатывать ПДн содержащие информацию о политических, религиозных и иных убеждениях и частной жизни, равно как ПДн о членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законодательством.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии с Конституцией Российской Федерации администрация и подразделения вправе получать и обрабатывать данные о частной жизни работников, только с их письменного согласия.

4.5. Хранение ПДн в администрации и подразделениях:

а) ПДн, содержащиеся на бумажных носителях, хранятся в запираемых шкафах, сейфах, установленных на рабочих местах лиц, уполномоченных на обработку ПДн;

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 администрации и подразделениях.

4.6. Хранение документов содержащих ПДн, а так же передача их для хранения в специализированные учреждения осуществляется в соответствии с действующим законодательством Российской Федерации, законодательством Белгородской области, правовыми актами администрации города Белгорода.

5. Доступ к персональным данным

5.1. К ПДн в администрации и подразделениях имеют доступ лица, указанные в перечне уполномоченных на обработку ПДн.

5.2. В целях выполнения порученного задания (служебных обязанностей) и на основании служебной записки с положительной резолюцией руководителя структурного подразделения, в котором обрабатываются ПДн, доступ на определенный срок к ПДн может быть предоставлен иному работнику администрации или подразделения, должность которого не включена в перечень лиц, уполномоченных на обработку ПДн и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих ПДн.

5.3. Уполномоченные лица на обработку ПДн имеют право получать только те ПДн, которые необходимы им для выполнения конкретных функций в соответствии с их должностной инструкцией.

5.4 Субъекты ПДн, хранящихся в администрации и подразделениях, имеют право на свободный доступ к своим ПДн, включая право на получение копии любой записи (за исключением случаев предусмотренных федеральным законодательством), содержащей их ПДн. Субъекты ПДн имеют право требовать внесения изменений в свои данные в случае обнаружения в них неточностей.

5.5. Работники администрации и подразделений, уполномоченные на обработку ПДн, в связи с исполнением трудовых обязанностей, обеспечивают хранение информации, содержащей ПДн, исключающее доступ к ним третьих лиц.

5.6. В период отпуска, служебной командировки и иных случаях длительного отсутствия работника администрации или подразделения на рабочем месте, работник заранее обязан передать документы и иные носители, содержащие ПДн лицу, на которое приказом руководителя будет возложено исполнение его трудовых обязанностей.

В случае если такое лицо не назначено, то документы и иные носители, содержащие ПДн передаются уполномоченному лицу на обработку ПДн, по указанию руководителя.

При увольнении уполномоченного лица на обработку ПДн, документы и иные носители, содержащие ПДн, передаются другому уполномоченному лицу на обработку ПДн, по указанию руководителя.

5.7. Процедура оформления доступа к ПДн работника администрации, подразделения, включает в себя:

- ознакомление под роспись с настоящим положением и иными нормативными актами, регулирующими обработку и защиту ПДн в администрации и подразделениях;

- истребование письменного обязательства о соблюдении конфиденциальности ПДн и соблюдении правил их обработки.

5.8. Передача (обмен и т.д.) ПДн в администрации и подразделениях осуществляется только между уполномоченными лицами на обработку ПДн, в рамках исполнения своих должностных обязанностей и инструкций.

5.9. Передача ПДн хранящихся в администрации и подразделениях, третьим лицам осуществляется только с их письменного согласия.

Согласие субъектов ПДн, 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 на основании заключенных договоров, а также в случаях, установленных Федеральным законом от 27 июня 2006 г. № 152-ФЗ «О персональных данных».

5.10. Не допускается передача ПДн в коммерческих целях без письменного согласия субъекта ПДн.

5.11. Работники администрации и подразделений, 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 полученных ПДн лишь в целях, для которых они сообщены;

- 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, государственного или муниципального контракта, поручение оператора, где должен быть предусмотрен перечень действий, устанавливающий соблюдение конфиденциальности ПДн и обеспечение безопасности ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона от 27.07.2006 №152 «О персональных данных»;

- соглашения о неразглашении ПДн либо наличия в договоре с третьим лицом пунктов о неразглашении ПДн.

При иных обстоятельствах передачи документов содержащих ПДн, третьим лицам, необходимо наличие письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей ПДн, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

Ответственность за соблюдение порядка предоставления ПДн третьим лицам несет лицо, уполномоченное на обработку ПДн.

5.12. Представителю субъекта ПДн, в том числе работника администрации или подразделения, ПДн передаются в порядке, установленном действующим законодательством и настоящим положением.

Информация передается при наличии одного из документов:

- нотариально заверенной доверенности представителя;
- письменного заявления работника, написанного в присутствии ответственного лица, допущенного к обработке ПДн.

Доверенности и заявления хранятся в структурных подразделениях, обрабатывающих запрашиваемые ПДн работников.

5.13. ПДн могут быть предоставлены родственникам или членам семьи субъекта ПДн, только с письменного разрешения субъекта ПДн, за исключением случаев, когда передача ПДн без согласия допускается действующим законодательством Российской Федерации.

5.14. Доступ к электронным базам данных, содержащим ПДн, обеспечиваются системой паролей. Система паролей и лицо ответственное за соблюдение системы паролей определяются дополнительным локальным нормативным актом оператора ПДн.

5.15. Запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений (при наличии такого функционала). Содержание электронного журнала обращений проверяется не реже 1 раза в месяц ответственным лицом за организацию обработки персональных данных.

5.16. Федеральным законом от 27 июня 2006 г. № 152-ФЗ «О персональных данных» предусмотрена трансграничная передача ПДн, которая может осуществляться на территории иностранных государств в следующих случаях:

1. Наличия согласия в письменной форме субъекта ПДн;
2. Предусмотренных международными договорами Российской Федерации;
3. Предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства;
4. Исполнения договора, стороной которого является субъект ПДн;

5. Защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

6. Защита персональных данных в администрации и подразделениях

6.1. Защита ПДн от неправомерного их использования или утраты обеспечивается администрацией, подразделением в порядке, установленном федеральным законодательством.

6.2. Общую организацию защиты ПДн в администрации и подразделениях осуществляют их руководители.

6.3. Лицо ответственное за организацию обработки ПДн организует:

- ознакомление с настоящим положением под роспись работников, уполномоченных на обработку ПДн;
- в случае вступления в силу иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных работников администрации и подразделений, также производится ознакомление под роспись;
- истребование с работников, имеющих доступ к ПДн администрации и подразделений письменного обязательства о соблюдении конфиденциальности ПДн в администрации и подразделениях и соблюдении правил их обработки. Обязательство разрабатывается оператором ПДн в соответствии со статьей 7 Федерального закона от 27.07.2006 №152 «О персональных данных».

6.4. В целях обеспечения защиты ПДн, хранящихся в электронных базах данных администрации и подразделений, от НСД, искажения и уничтожения ПДн, 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 (при наличии функционала);

- 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 помощью их маркировки и занесение учетных данных в журнал учета;

- 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 вредоносных программ (программ - вирусов) и программных закладок.

6.5. При взаимодействии ИСПДн с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования), применяются следующие методы 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.

6.6. С целью получения общедоступной информации, 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.

6.7. При удаленном доступе к информационной системе через информационно - телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования), 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.

6.8. При межсетевом взаимодействии отдельных информационных систем через информационно - телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования), 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).

6.9. При межсетевом взаимодействии отдельных информационных систем разных операторов через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования), 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.

6.10. 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 установленном 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.

6.11. Организация выполнения методов и способов защиты информации, назначение ответственных лиц определяется локальным актом администрации, подразделения.

6.12. 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.

6.13. 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.

6.14. Для защиты персональных данных в ИСПДн привлекаются для выполнения специальных, аналитических и экспертных работ по защите информации специализированные организации-лицензиаты ФСТЭК и ФСБ России, имеющие право на деятельность по защите информации (проведение контроля отсутствия не декларированных возможностей, аттестации технических средств, установки необходимых средств защиты информации).

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

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

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

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

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

6.16. При обработке ПДн в информационной системе руководителями администрации и подразделений, должны обеспечиваться:

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

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

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

6.17. Каждый съемный носитель, с записанными на нем ПДн, должен иметь маркировку, на которой указывается его уникальный учетный номер. Ответственность за учет съемных носителей ПДн лежит на работниках, уполномоченных на обработку ПДн. Выдачу съемных носителей ПДн лицам, уполномоченных на обработку ПДн, осуществляют ответственные за организацию обработки ПДн. Учет носителей ПДн осуществляется в журнале учета съемных носителей ПДн.

6.18. В случае выхода из строя техники, на которой проводилась обработка ПДн, её вынос за пределы территории администрации и подразделений с целью ремонта, замены и т.п. без согласования с руководителем или назначенным ответственным лицом за защиту информации из числа работников администрации и подразделений, или специалистами отдела по защите информации администрации и подразделений (далее – ответственные работники за защиту информации) в администрации и подразделениях запрещается.

6.19. Съемные носители ПДн, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению по акту. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией, утвержденной локальным актом администрации, подразделения. По результатам уничтожения носителей составляется акт, при необходимости уничтожения информации с носителей ПДн также составляется акт.

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

7.1. Права, обязанности, действия лиц, в трудовые обязанности которых входит обработка ПДн работников администрации и подразделений, определяются их должностными инструкциями.

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

Начальник управления делами
аппарата администрации города **А.Д. Ковальчук**