АДМИНИСТРАЦИЯ ГОРОДА ЖЕРДЕВКА
ЖЕРДЕВСКОГО РАЙОНА ТАМБОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

14.04.2017 г. Жердевка № 205

Об утверждении Положения о порядке организации и проведения работ по обработке и защите конфиденциальной информации

В целях организации проведения работ по обработке и обеспечению защиты информации ограниченного доступа, не составляющей государственную тайну, администрация области постановляет:

1. Утвердить Положение о порядке организации и проведения работ по обработке и защите конфиденциальной информации согласно приложению.
2. Настоящее постановление опубликовать на сайте сетевого издания «ТОП68 Тамбовский областной портал» (www.top68.ru)
3. Контроль за исполнением настоящего постановления оставляю за собой

Глава администрации города В.А. Соловьев

УТВЕРЖДЕНО
постановлением администрации города
от 14.04.2017 № 205

Положение
о порядке организации и проведения работ по обработке и защите конфиденциальной информации

1. Общие положения

1.1. Положение о порядке организации и проведения работ по обработке и защите конфиденциальной информации (далее - Положение) определяет общий порядок обращения с документами на бумажном носителе, а также другими материальными носителями информации (фото-, кино-, аудио-, видео-, машинными носителями, физическими полями), содержащими информацию ограниченного доступа, в администрации города, в органах исполнительной власти города, а также в подведомственных им предприятиях и учреждениях (далее - органы, организации).

1.2. Информация ограниченного доступа по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную. В соответствии с федеральным законодательством к конфиденциальной информации относятся сведения, составляющие служебную тайну (служебная информация ограниченного доступа), профессиональную тайну, коммерческую тайну, банковскую тайну, персональные данные.

1.3. К служебной информации ограниченного доступа относится несекретная информация, касающаяся деятельности органов, организаций, ограничения на доступ к которой диктуются служебной необходимостью.

1.4. Защита конфиденциальной информации осуществляется на основе Конституции Российской Федерации, требований Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (в редакции от 28.12.2013), других законодательных актов Российской Федерации:

1.4.1. организация и проведение работ по защите служебной информации ограниченного доступа, отнесенной к государственным информационным ресурсам, при ее обработке техническими средствами определяется приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";

1.4.2. организация и проведение работ по защите персональных данных

определяется на основе Трудового кодекса Российской Федерации, требований Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (в редакции от 23.07.2013), постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", постановления Правительства Российской Федерации от 21 марта 2012 г. № 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", постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

1.5. Информационные ресурсы, содержащие конфиденциальную информацию, сформированные в процессе деятельности органов власти, а также приобретенные в государственную собственность Тамбовской города установленными законодательством Российской Федерации способами, являются государственной собственностью Тамбовской города и не могут быть использованы иначе как с разрешения собственника или в установленных законодательством Российской Федерации случаях.

1.6. Отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации.

1.7. Для определения конфиденциальности сведений используется перечень сведений конфиденциального характера, составленный в соответствии с федеральным законодательством.

1.8. Законодательством Российской Федерации запрещено относить к информации ограниченного доступа:

законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к

государственной тайне;

документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти города, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

1.9. Информация конфиденциального характера не может быть использована в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан.

1.10. В случае ликвидации органа, организации решение о дальнейшем использовании служебной информации ограниченного доступа принимает ликвидационная комиссия.

1.11. Положение не распространяется на порядок обращения со сведениями, составляющими государственную тайну.

2. Обязанности должностных лиц органа, организации по защите информации конфиденциального характера и ответственность за разглашение конфиденциальной информации

2.1. Должностные лица органа, организации обязаны принимать меры по защите информации конфиденциального характера.

2.2. Руководитель органа, организации в пределах своей компетенции определяет:

порядок подготовки, учета, хранения и уничтожения документов и электронных носителей с конфиденциальной информацией;

порядок обработки конфиденциальной информации с помощью средств электронно-вычислительной техники;

порядок передачи информации конфиденциального характера другим органам, организациям, а также между структурными подразделениями своего органа, организации;

категории должностных лиц, уполномоченных относить информацию к разряду ограниченного доступа;

порядок снятия пометки "Для служебного пользования" (далее - ДСП) с носителей информации ограниченного доступа;

основные мероприятия защиты конфиденциальной информации.

2.3. Должностные лица органа, организации, принявшие решение об отнесении служебной информации к разряду ограниченного доступа, несут персональную ответственность за принятие необоснованного решения и за несоблюдение ограничений, предусмотренных пунктом 1.8 Положения.

2.4. При поступлении на государственную гражданскую службу города государственный гражданский служащий города, работник организации (далее - работник) предупреждается об ответственности за разглашение сведений конфиденциального характера, ставших ему известными в связи с выполнением

им своих служебных обязанностей.

2.5. Допуск к конфиденциальной информации предусматривает в служебном контракте (трудовом договоре) обязательства работника перед работодателем по нераспространению доверенной конфиденциальной информации.

2.6. Доступ исполнителей (пользователей) к конфиденциальной информации осуществляется в соответствии с разрешительной системой допуска исполнителей к документам и сведениям ограниченного доступа.

2.7. Конфиденциальная информация без санкции соответствующего должностного лица органа, организации не подлежит разглашению (распространению).

2.8. Работники не могут использовать в личных целях сведения конфиденциального характера, ставшие им известными вследствие выполнения служебных обязанностей.

2.9. За разглашение конфиденциальной информации, а также нарушение порядка обращения с документами, содержащими такую информацию, работник может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

3. Порядок обращения с документами и электронными носителями информации, содержащими конфиденциальную информацию

3.1. Конфиденциальная информация, содержащаяся в документах, имеющих обращение в органе, организации, является служебной информацией ограниченного доступа.

3.2. Учет документов конфиденциального характера осуществляется в соответствии с разрабатываемой в органе, организации инструкцией по делопроизводству.

3.3. На документах, содержащих конфиденциальную информацию, проставляется пометка "ДСП".

3.4. Указанная пометка и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к таким документам.

3.5. Прием и учет (регистрация) документов, содержащих информацию конфиденциального характера, осуществляются структурным подразделением органа, организации, которому поручен прием и учет несекретной документации.

3.6. Документы с пометкой "ДСП":

учитываются поэкземплярно;

печатаются в служебном помещении, в котором выполнен комплекс мер по технической защите информации. На обороте последнего листа каждого экземпляра документа указывается количество отпечатанных экземпляров, фамилия исполнителя документа, фамилия лица, напечатавшего документ, и дата печатания документа. Отпечатанные и подписанные документы вместе с черновиками передаются для регистрации работнику, ответственному за их учет. Черновики уничтожаются этим работником с отражением факта уничтожения в учетных формах;

учитываются отдельно от несекретной документации. При незначительном объёме таких документов разрешается вести их учет совместно с другими несекретными документами. К регистрационному номеру документа добавляется пометка "ДСП". Регистрационный номер и дата учета документа указываются в установленном месте углового штампа бланка органа, организации или проставляется в левом верхнем углу первой страницы документа;

передаются работникам структурных подразделений органа, организации под расписку;

пересылаются сторонним органам, организациям фельдъегерской (специальной) связью, заказными или ценными почтовыми отправлениями;

размножаются (тиражируются) только с письменного разрешения соответствующего руководителя органа, организации. Учет размноженных документов осуществляется поэкземплярно;

хранятся в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах).

3.7. При необходимости направления документов с пометкой "ДСП" в несколько адресов составляется указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов.

Указатель рассылки подписывается руководителем структурного подразделения органа, организации, готовившего документ.

3.8. Исполненные документы с пометкой "ДСП" группируются в дела в соответствии с номенклатурой дел несекретного делопроизводства. При этом на обложке дела, в которое помещены такие документы, также проставляется пометка "ДСП".

3.9. Уничтожение дел, документов с пометкой "ДСП", утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

3.10. Передача документов и дел с пометкой "ДСП" от одного работника другому осуществляется с разрешения соответствующего руководителя органа, организации.

3.11. При смене работника, ответственного за учет документов с пометкой "ДСП", составляется акт приема-передачи этих документов, который утверждается соответствующим руководителем органа, организации.

3.12. Проверка наличия документов, дел, изданий с пометкой "ДСП" проводится не реже одного раза в год комиссией, создаваемой руководителем органа, организации. В состав такой комиссии обязательно включается работник(и), ответственный(е) за учет и хранение этих материалов.

3.13. В архивах, где сосредоточено большое количество изданий, дел и других материалов с пометкой "ДСП", проверка наличия может проводиться не реже одного раза в пять лет. Результаты проверки оформляются актом.

3.14. 0 фактах утраты документов, дел и изданий, содержащих конфиденциальную информацию, либо разглашения этой информации ставится в известность руководитель органа, организации, который назначает комиссию для

расследования обстоятельств утраты или разглашения. Результаты расследования докладываются руководителю, назначившему комиссию.

На утраченные документы, дела и издания с пометкой "ДСП" составляется акт, на основании которого делаются соответствующие отметки в учетных формах. Акты на утраченные дела постоянного срока хранения после их утверждения передаются в архив для включения в дело фонда.

3.15. При снятии пометки "ДСП" на документах, делах или изданиях, а также в учетных формах делаются соответствующие отметки и информируются все адресаты, которым эти документы (издания) направлялись.

3.16. Электронные носители, содержащие конфиденциальную информацию:

учитываются структурным подразделением органа, организации, которому поручен учет и прием несекретной документации по журналу учета машинных носителей информации. Учетные реквизиты (учетный номер, дата регистрации, пометка "ДСП") проставляются на электронных носителях информации в удобном для просмотра месте;

передаются другим исполнителям под расписку в журнале учета машинных носителей информации или по карточке учета;

уничтожаются по акту.

3.17. Порядок рассылки, уничтожения, передачи, проверки наличия электронных носителей информации, проведения расследований по фактам утраты электронных носителей информации, снятия пометки "ДСП" с электронных носителей информации и так далее является таким же, как и для документов конфиденциального характера на бумажном носителе.

4. Порядок обмена информацией конфиденциального характера

4.1. Информация конфиденциального характера не подлежит распространению (передаче) без санкции соответствующего руководителя органа, организации.

4.2. Документированная информация конфиденциального характера, сформированная в процессе деятельности органа, организации за счет средств местного бюджета, а также приобретенная в государственную собственность города установленными законодательством Российской Федерации способами, предоставляется органам государственной власти города, областным государственным учреждениям, предприятиям, органам местного самоуправления на безвозмездной основе.

4.3. Передача указанной выше конфиденциальной информации иным пользователям, если иное не установлено законодательством, должна регулироваться договорными отношениями, предусматривающими обязательства и ответственность сторон, перечень сведений, являющихся конфиденциальными и компенсацию за нарушение договорных обязательств.

5. Организация и проведение работ по защите конфиденциальной информации

5.1. Организация и проведение работ по защите конфиденциальной информации при ее обработке техническими средствами определяются Положением, действующими государственными стандартами, методическими документами Федеральной службы по техническому и экспортному контролю.

5.2. Защита конфиденциальной информации осуществляется путем выполнения комплекса мероприятий (правовых, организационных, технических) по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Правительством Российской Федерации и федеральными органами исполнительной власти, уполномоченными в города обеспечения безопасности, противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

5.3. Организация работ по защите конфиденциальной информации возлагается на руководителя органа, организации, руководителей структурных подразделений органа, организации, осуществляющих разработку проектов объектов информатизации и их эксплуатацию, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации - на руководителя структурного подразделения по защите информации органа, организации, а в случае их отсутствия, на нештатного ответственного за безопасность информации, назначаемого из числа наиболее подготовленных работников.

5.4. Лица, осуществляющие обработку информации конфиденциального характера на средствах вычислительной техники (далее - СВТ), несут ответственность за несоблюдение ими порядка обращения с конфиденциальной информацией.

5.5. В органе, организации разрабатываются нормативные правовые акты по организации защиты информации,

5.6. При необходимости состав проводимых мероприятий по защите информации может быть дополнен в соответствии с решаемыми задачами и конкретными условиями применения СВТ.

5.7. Для обработки конфиденциальной информации необходимо использовать СВТ в защищенном исполнении с применением сертифицированных программных, технических и программно-технических средств защиты информации. Вычислительные комплексы обработки информации должны быть аттестованы по требованиям безопасности информации. Применяемое программное обеспечение - лицензионным.

5.8. Для передачи конфиденциальной информации по линиям связи, выходящим за пределы контролируемой зоны органа, организации, необходимо использовать защищенные каналы связи (средства криптографической защиты

информации).

5.9. При проектировании вновь создаваемых автоматизированных систем (далее - АС) на базе СВТ перечень требований по защите информации отражается в разделе "Специальные требования по защите информации" технического задания на создание АС. Требования по защите информации разрабатываются одновременно с другими разделами технического задания с привлечением работников структурного подразделения органа, организации по защите информации.