



АДМИНИСТРАЦИЯ ГОРОДА ЮЖНО-САХАЛИНСКА

ПОСТАНОВЛЕНИЕ

от 26.05.2014 № 903-па

Об упорядочении обращения со служебной информацией ограниченного распространения в администрации города Южно-Сахалинска

В целях упорядочения обращения со служебной информацией ограниченного распространения в администрации города Южно-Сахалинска, отраслевых (функциональных) органах, муниципальных казенных и бюджетных учреждениях, муниципальных унитарных предприятиях, администрация города Южно-Сахалинска **постановляет**:

1. Утвердить:
 - 1.1. Категории должностных лиц администрации города Южно-Сахалинска, уполномоченных относить служебную информацию к разряду ограниченного распространения (прилагаются);
 - 1.2. Перечень служебной информации ограниченного распространения в администрации города Южно-Сахалинска (прилагается);
 - 1.3. Инструкцию о порядке обращения со служебной информацией ограниченного распространения в администрации города Южно-Сахалинска (прилагается);
 - 1.4. Положение об организации защиты служебной информации ограниченного распространения в администрации города Южно-Сахалинска (прилагается).
2. Руководителям структурных подразделений аппарата администрации города, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, унитарных предприятий, ознакомить подчиненных им сотрудников с настоящим постановлением и обеспечить его исполнение.
3. Признать утратившими силу :
 - постановление мэра города Южно-Сахалинска от 16.11.2004 № 55дсп «Об утверждении Положения о порядке обращения со сведениями конфиденциального характера в органах местного самоуправления муниципального образования «город Южно-Сахалинск»;

- постановление мэра города Южно-Сахалинска от 27.04.2005 № 824 «Об утверждении Положения о порядке организации работ по защите конфиденциальной информации в администрации города Южно-Сахалинска».

4. Разместить настоящее постановление на официальном сайте администрации города Южно-Сахалинска.

5. Контроль исполнения постановления администрации города возложить на вице-мэра, руководителя аппарата.

Исполняющий обязанности мэра города

С.А.Надсадин

УТВЕРЖДЕНЫ
постановлением администрации
города Южно-Сахалинска
от 26.05.2014 № 903-па

**КАТЕГОРИИ ДОЛЖНОСТНЫХ ЛИЦ,
УПОЛНОМОЧЕННЫХ ОТНОСИТЬ СЛУЖЕБНУЮ ИНФОРМАЦИЮ
К РАЗРЯДУ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ**

1. Мэр города;
2. Первый вице-мэр, вице-мэры;
3. Руководители структурных подразделений аппарата администрации города;
4. Руководители отраслевых (функциональных) органов;
5. Руководители муниципальных казенных учреждений;
6. Руководители муниципальных бюджетных учреждений;
7. Руководители муниципальных унитарных предприятий.

Начальник Управления мобилизационной
подготовки и защиты информации

В.В.Кочкин

УТВЕРЖДЕН
постановлением администрации
города Южно-Сахалинска
от 26.05.2014 № 903-па

**ПЕРЕЧЕНЬ
СЛУЖЕБНОЙ ИНФОРМАЦИИ ОГРАНИЧЕННОГО
РАСПРОСТРАНЕНИЯ В АДМИНИСТРАЦИИ
ГОРОДА ЮЖНО-САХАЛИНСКА**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Перечень разработан в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», другими нормативными правовыми актами в области использования и защиты информационных ресурсов и предназначен для муниципальных служащих (работников) аппарата администрации города, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, унитарных предприятий, выполнение должностных обязанностей которых связано с использованием сведений, содержащих служебную информацию ограниченного распространения.

1.2. Настоящий Перечень не ограничивает должностных лиц, категории которых утверждены постановлением администрации города от __.__.____ № _____, в праве отнесения документированной информации к сведениям ограниченного распространения, устанавливая при этом на документах гриф «Для служебного пользования», если такое ограничение вызвано служебной необходимостью и не запрещено законодательством Российской Федерации.

1.3. Документированная информация, входящая в настоящий Перечень, должна быть помечена грифом «Для служебного пользования» в соответствии с Инструкцией о порядке обращения со служебной информацией ограниченного распространения в администрации города Южно-Сахалинска, утвержденной постановлением администрации города от __.__.____ № _____.

1.4. В настоящем Перечне используются следующие понятия и сокращения:

ГО - гражданская оборона;

ЕМТС – единая мультисервисная телекоммуникационная сеть администрации города;

Организация - орган государственной власти или местного самоуправления, а также учреждение, предприятие или организация, объединение независимо от их организационно-правовой формы и формы собственности.

1.5. Для однозначной трактовки содержания настоящего Перечня принимается следующее:

- при перечислении сведений через союз «и», гриф «Для служебного пользования» устанавливается всем сведениям в совокупности;
- при перечислении сведений через запятую и союз «или», гриф «Для служебного пользования» устанавливает как для каждого сведения в отдельности, так и всем сведениям в совокупности;
- при перечислении сведений после словосочетания «по совокупности» через запятую, союзы «и» и «или», гриф «Для служебного пользования» устанавливается только всем сведениям в совокупности;
- со словосочетания «а также» начинаются новые сведения, которые отличны от предыдущих и которым в отдельности также устанавливается гриф «Для служебного пользования».

2. СВЕДЕНИЯ, СОДЕРЖАЩИЕ СЛУЖЕБНУЮ ИНФОРМАЦИЮ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ В АДМИНИСТРАЦИИ ГОРОДА ЮЖНО-САХАЛИНСКА

2.1. Военно-мобилизационные вопросы, вопросы гражданской обороны.

2.1.1. Сведения по вопросам мобилизационной подготовки, не раскрывающие обобщенные данные в целом по городу, организации.

2.1.2. Сведения по наличию запасов мобилизационного резерва в отдельных организациях, не раскрывающие обобщенные данные в целом по городу, организации.

2.1.3. Сведения о наличии в определенных организациях защитных сооружений ГО, средств индивидуальной защиты ГО, специальных формирований ГО, переписка, принимаемые решения по этим вопросам, не раскрывающие обобщенных данных в целом по городу, организации.

2.1.4. Сведения по испытанию защитных или специальных сооружений ГО на соответствие санитарно-гигиеническим и санитарно-техническим нормам.

2.1.5. Сведения по учету и бронированию военнообязанных по отдельным организациям, в которых работает военнообязанных менее 300 человек.

2.1.6. Аналитические справки, письма, телеграммы и другие материалы по мобилизационной подготовке, не раскрывающие задания на расчетный год, объемы оборонной продукции, наличие и наращивание мощностей по ее выпуску, сведения по учету и бронированию граждан, пребывающих в запасе.

2.1.7. Образцы форм представляемых сведений по мобилизационной подготовке на расчетный год.

2.1.8. Сведения о согласовании объемов мобилизационных заданий с организациями для нужд органов государственной власти и органов местного самоуправления.

2.2. Вопросы экономической деятельности и внешнеэкономических связей.

2.2.1. Сведения о подготовке к торгам (тендерам, конкурсам, аукционам), содержащие расчетные материалы, справки, предложения, за исключением сведений, подлежащих обязательному опубликованию при проведении торгов (тендеров, конкурсов, аукционов).

2.2.2. Нормативные, расчетные материалы, справки по ценам на продукцию, завозимую в соответствии с внешнеэкономическими контрактами.

2.2.3. Нормативные, расчетные материалы, справки по ценам на продукцию, поступающую по линии гуманитарной помощи.

2.2.4. Сведения о результатах текущей деятельности.

2.2.5. Балансы ресурсов и использования основных видов продовольственных ресурсов.

2.2.6. Бухгалтерские документы согласно Федеральному закону от 06 декабря 2011 г. № 402-ФЗ «О бухгалтерском учете».

2.2.7. Сводные данные о финансировании, реестры и платежные документы на оплату договоров о производственной и финансовой деятельности.

2.3. Жилищно-коммунальное хозяйство.

2.3.1. Сведения по совокупности об источниках водоснабжения, а именно количество воды, дебет источника, соответствие источника текущим и прогнозируемым потребностям населения.

2.3.2. Технологические схемы муниципальных или ведомственных водозаборов, проектные сведения по их строительству.

2.3.3. Сведения по совокупности о системах подачи и распределения воды, в том числе производственного или промышленного водоснабжения в целом по городу, а именно материал, год постройки, степень износа, протяженность по каждому характерному признаку.

2.3.4. Сведения по совокупности об источниках электроснабжения, их технических характеристиках и сведения об их топографической привязке к местности в целом по городу.

2.3.5. Сведения по совокупности об инженерной инфраструктуре города, схемах их тепловых и электрических сетей, трансформаторных подстанций.

2.3.6. Сведения по совокупности о наличии санитарно-обмывочных пунктов, на базе чего они созданы, их пропускной способности по городу в целом.

2.3.7. Сведения по совокупности о наличии станций обеззараживания одежды, на базе чего они созданы, их пропускной способности по городу в целом.

2.3.8. Сведения по совокупности о наличии станций обеззараживания территорий, на базе чего они созданы, их пропускной способности по городу в целом.

2.4. Проектирование, геодезия и картография

2.4.1. Чертежи генеральных планов и проектов детальной планировки города.

2.4.2. Пояснительные записки к генеральным планам, концепциям генеральных планов, проектам детальной планировки города и зон отдыха.

2.4.3. Пояснительные записки (по типу основных положений) к схемам и проектам районных планировок, к проектам районных планировок промышленных районов, схемам генеральных планов промышленных узлов.

2.4.4. Каталоги, списки координат геодезических пунктов и географических объектов в местной системе координат или системе координат 1963 года, составленные на участок местности в пределах территории города или площадью до 5000 кв.км.

2.5. Персональные данные.

2.5.1. Сведения, содержащиеся в книгах записей актов гражданского состояния или в метрических книгах церквей, миссий о рождении, заключении брака, расторжении брака, смерти, усыновлении, установлении отцовства, перемене фамилии, имени, отчества.

2.5.2. Списки со сведениями на детей (от 0 до 18 лет), оставшихся без попечения родителей и подлежащих устройству в семью (передаче под опеку, на усыновление, удочерение), с указанием индивидуальных внешних данных и психологических характеристик детей, медицинских сведений, данных о месте и времени рождения, родителях, обстоятельствах лишения родительских прав.

2.5.3. Индивидуальные медицинские карты на детей (от 0 до 18 лет), оставшихся без попечения родителей и подлежащих устройству в семью (передаче под опеку, на усыновление, удочерение).

2.5.4. Анкеты со сведениями на детей (от 0 до 18 лет), оставшихся без попечения родителей и подлежащих устройству в семью (передаче под опеку, на усыновление, удочерение).

2.5.5. Документированная информация, содержащая сведения о фактах, событиях и обстоятельствах частной жизни граждан, позволяющая идентифицировать их личность, за исключением сведений, подлежащих распространению в средствах массовой информации в соответствии с законодательством Российской Федерации.

2.5.6. Персональные данные (личные дела) муниципальных служащих (работников) аппарата администрации города, отраслевых (функциональных)

органов, муниципальных казенных и бюджетных учреждений, унитарных предприятий.

2.5.7. Персональные данные получателей доплат к пенсиям, иной адресной социальной помощи.

2.5.8. Персональные данные о лицах, участвовавших в вооруженных конфликтах.

2.6. Информатизация и защита информационных ресурсов.

2.6.1. Схемы соединений технических средств обработки информации, объединенных в ЕМТС с указанием технологических параметров или технических характеристик и мест расположения составных элементов.

2.6.2. Сведения о методах, средствах, эффективности защиты информационных ресурсов ЕМТС от разрушения, искажения, утечки или несанкционированного доступа в процессе создания информации, ее обработки, хранения и распространения в ЕМТС, средствах вычислительной техники, а также в помещениях и вне их.

2.6.3. Сведения о состоянии защищенности информационных ресурсов, в том числе сведения, содержащие отчетные материалы, тематику проводимых или планируемых мероприятий по обеспечению информационной безопасности.

2.6.4. Сведения о расположении и конфигурировании серверов ЕМТС, баз данных, информационных порталов.

2.7. Прочие сведения.

2.7.1. Штатное расписание аппарата администрации города, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий.

2.7.2. Полный список номеров телефонов, включая домашние и мобильные, сотрудников аппарата администрации города, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, унитарных предприятий с указанием занимаемых должностей.

2.7.3. Полные сведения реестра по учету муниципального имущества.

2.7.4. Итоговые (сводные) материалы результатов служебных проверок, проводимых в аппарате администрации города, отраслевых (функциональных) органах, муниципальных казенных и бюджетных учреждениях, муниципальных унитарных предприятиях.

2.7.5. Акты проведения ревизий и проверок, постановления, распоряжения администрации города, служебные письма, запросы, раскрывающие конфиденциальные сведения о проверяемых предприятиях, организациях, юридических и физических лицах. Планы проведения ревизий и проверок.

2.7.6. Сведения о передаче служебной (конфиденциальной) информации в территориальные органы федеральных органов исполнительной власти, органы власти Сахалинской области, другие организации.

2.7.7. Перечни сведений, отнесенных к служебной (конфиденциальной) информации территориальных органов федеральных органов исполнительной власти, органов власти Сахалинской области, других организации, используемых в своей деятельности структурными подразделениями аппарата администрации города, отраслевыми (функциональными) органами, муниципальными казенными и бюджетными учреждениями, муниципальными унитарными предприятиями.

2.7.8. Сведения ограниченного распространения о проводимых антитеррористических мероприятиях (за исключением сведений, относящихся к государственной тайне).

2.7.9. Сведения, поступившие от территориальных органов федеральных органов исполнительной власти, органов власти Сахалинской области, других органов местного самоуправления, организаций, физических и юридических лиц, доступ к которым ограничен в соответствии с федеральными законами, при наличии на документах, содержащих эти сведения, или сопроводительных документах, соответствующих пометок, указывающих на их служебный (конфиденциальный) характер.

2.7.10. Сведения, составляющие тайну следствия и судопроизводства.

2.7.11. Сведения, содержащие коммерческую тайну (т.е. связанные с коммерческой деятельностью), доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.

2.7.12. Другие сведения, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и иными федеральными законами.

2.7.13. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2.7.14. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и др.).

Начальник Управления мобилизационной
подготовки и защиты информации

В.В.Кочкин

УТВЕРЖДЕНА
постановлением администрации
города Южно-Сахалинска
от 26.05.2014 № 903-па

**ИНСТРУКЦИЯ
О ПОРЯДКЕ ОБРАЩЕНИЯ СО СЛУЖЕБНОЙ ИНФОРМАЦИЕЙ
ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ В АДМИНИСТРАЦИИ
ГОРОДА ЮЖНО-САХАЛИНСКА**

I. Общие положения

1.1. Настоящая Инструкция определяет порядок обращения с документами и другими материальными носителями информации, содержащими служебную информацию ограниченного распространения в аппарате администрации города Южно-Сахалинска, отраслевых (функциональных) органах, муниципальных казенных и бюджетных учреждениях, муниципальных унитарных предприятиях.

1.2. К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности аппарата администрации города Южно-Сахалинска, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий, ограничения на распространение которой диктуются служебной необходимостью.

1.3. Не могут быть отнесены к служебной информации ограниченного распространения:

нормативные правовые акты;

информация о состоянии окружающей среды;

информация о деятельности аппарата администрации города Южно-Сахалинска, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий, об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

информация, накапливаемая в открытых фондах библиотек и архивов, а также в муниципальных информационных системах, созданных или предназначенных для обеспечения граждан и организаций такой информацией;

иная информация, недопустимость ограничения доступа к которой установлена действующим законодательством.

1.4. На документах и выписках из них (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется гриф «Для служебного пользования».

1.5. Необходимость проставления грифа «Для служебного пользования» на документах, содержащих служебную информацию ограниченного распространения, определяется ответственным исполнителем и должностным лицом, подписывающим или утверждающим документ, а в отношении постановлений и распоряжений администрации города - руководителем структурного подразделения аппарата администрации города Южно-Сахалинска, отраслевого (функционального) органа, муниципального казенного и бюджетного учреждения, муниципального унитарного предприятия, готовившим соответствующий проект.

Перечень служебной информации ограниченного распространения в администрации города утвержден постановлением администрации города Южно-Сахалинска от __.__.____ № ____.

1.6. Должностные лица, принявшие решение об отнесении служебной информации к разряду служебной информации ограниченного распространения, несут персональную ответственность за обоснованность принятого решения и за соблюдение требований, предусмотренных пунктом 1.3 настоящей Инструкции.

1.7. Право отменить решение об отнесении документа к категории ограниченного распространения имеют должностные лица, которые приняли данное решение, либо вышестоящие по должности руководители.

1.8. Ответственность за организацию делопроизводства со служебной информацией ограниченного распространения, за соблюдение требований настоящей Инструкции, качественное и своевременное исполнение документов с грифом «Для служебного пользования» и их сохранность возлагается на руководителей структурных подразделений аппарата администрации города Южно-Сахалинска, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий.

1.9. Муниципальные служащие и работники аппарата администрации города Южно-Сахалинска, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий, отвечающие за учет (регистрацию), исполнение и хранение документов с грифом «Для служебного пользования», несут персональную ответственность за их сохранность, неразглашение информации ограниченного распространения и за соблюдение требований настоящей Инструкции.

За разглашение служебной информации ограниченного распространения, ее распространение без санкции должностного лица, имеющего данные полномочия, нарушение порядка обращения с документами или материальными носителями, содержащими такую

информацию, муниципальный служащий и работник аппарата администрации города Южно-Сахалинска, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий, может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

II. Порядок оформления служебных документов ограниченного распространения

2.1. Подготовка, оформление, прохождение и контроль исполнения документов с грифом «Для служебного пользования» осуществляются в соответствии с Инструкцией по делопроизводству в администрации города Южно-Сахалинска, утвержденной распоряжением администрации города Южно-Сахалинска от 12.08.2013 № 216-р, с учетом особенностей, установленных настоящей Инструкцией.

2.2. На служебных документах ограниченного распространения, приложениях к ним, делах и изданиях, содержащих сведения ограниченного распространения, проставляется гриф «Для служебного пользования». Указанный гриф и номер экземпляра проставляются в правом верхнем углу первой страницы документа, приложения к нему, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к таким документам. Например:

Для служебного пользования
Экз. № __

К регистрационному номеру документа добавляется пометка «ДСП».

2.3. На обороте последнего листа каждого экземпляра документа с грифом «Для служебного пользования» в левом нижнем углу исполнителем указывается регистрационный номер, количество отпечатанных экземпляров, расчет рассылки, фамилия исполнителя, фамилия печатавшего, дата печатания, служебный телефон исполнителя. Например:

уч. № 14 дсп		уч. № 14 дсп
Отп. - 2 экз.		Отп. - 8 экз.
Экз. № 1 - в адрес		Экз. N 1 - в дело
Экз. № 2 - в дело	или	Экз. N 2 - 8 - согласно
Исп. Смирнов В.В.		списку рассылки
Отп. Иванова М.И.		Исп. и отп. Иванов А.А.
01.02.2014		01.02.2014
498-272		(4242) 498-272

2.4. При отправке документов с пометкой «Для служебного пользования» с сопроводительным письмом после слова «Приложение» в письме указываются наименование каждого приложения, номер документа, номер экземпляра и количество листов.

2.5. Отпечатанные и подписанные документы вместе с черновиками передаются для регистрации и отправки ответственному лицу, осуществляющему учет и хранение документов с грифом «Для служебного пользования». Черновики уничтожаются указанным лицом путем измельчения в бумагорезательной машине.

III. Порядок учета и регистрации служебных документов ограниченного распространения

3.1. Прием и учет (регистрация) документов с грифом «Для служебного пользования», машинных носителей информации, содержащих электронные документы с информацией ограниченного распространения, осуществляют муниципальные служащие и работники структурных подразделений аппарата администрации города Южно-Сахалинска, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий, на которых возложены данные обязанности, в порядке, предусмотренном для общего делопроизводства с учетом особенностей, установленных настоящей Инструкцией.

3.2. Документы с грифом «Для служебного пользования» учитываются отдельно от другой служебной документации и регистрируются в специальном журнале по форме согласно приложению № 1 к настоящей Инструкции.

При незначительном объеме таких документов в структурных подразделениях аппарата администрации города Южно-Сахалинска, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий, разрешается вести их учет совместно с другими служебными документами, выделив отдельный раздел в журналах учета.

3.3. При регистрации входящего документа с грифом «Для служебного пользования» на первом листе в нижней его части с правой стороны ставится штамп, в котором указываются очередной порядковый номер документа и дата его поступления. К регистрационному номеру документа добавляется пометка «ДСП». Например:

входящий № 58 ДСП 01.02.2014

3.4. На сброшюрованных материалах входящие номера проставляются на титульном листе.

3.5. На машинных носителях информации учетные реквизиты (учетный номер, дата регистрации, пометка «ДСП») проставляются в удобном для просмотра месте.

Рассылка, передача, проверка наличия машинных носителей информации ограниченного распространения, проведение служебных проверок по фактам их утраты осуществляются в соответствии с пунктами 4.4, 4.5, 4.9, 6.5 и 6.6 настоящей Инструкции.

IV. Порядок размножения, рассылки (отправки), копирования и ознакомления со служебными документами ограниченного распространения

4.1. Размножение, копирование, ознакомление, передача и отправка документов с грифом «Для служебного пользования» производятся только с письменного разрешения должностного лица, в чей адрес был направлен документ, должностного лица, подписавшего или утвердившего документ, либо вышестоящего по должности руководителя.

4.2. Учет размноженных документов осуществляется поэкземплярно. Дополнительно размноженные экземпляры документа учитываются за номером этого документа, о чем делается отметка на размножаемом документе. Нумерация дополнительно размноженных экземпляров производится от последнего номера ранее учтенных экземпляров.

4.3. Копирование документов с грифом «Для служебного пользования» осуществляется в условиях, исключающих несанкционированный доступ к копируемым документам. На обороте последнего листа оригинала делается запись о количестве снятых копий и где они учтены, заверяемая специалистом, осуществляющим регистрацию документа, с проставлением даты. На копиях под номером экземпляра ставится номер копии, например:

Для служебного пользования
Экз. № 35
Копия № 1

4.4. К документу, предназначенному для направления в более чем четыре адреса, прилагается список рассылки, оформленный согласно приложениям № 2 или № 3 к настоящей Инструкции.

4.5. На пакетах (конвертах), в которых отправляются документы или машинные носители информации с грифом «Для служебного пользования», в правом верхнем углу проставляются гриф «Для служебного пользования»,

подпись лица, производившего конвертование, заверенная печатью «Для пакетов».

На упаковке (конверте) в последовательности, установленной правилами оказания услуг почтовой связи, указываются элементы почтового адреса, наименования получателя и отправителя, номера вложенных документов с добавлением отметки «ДСП». Запрещается указывать фамилии и должности руководителей структурных подразделений аппарата администрации города Южно-Сахалинска, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий. После того как конверт заклеен, на центр оборотной стороны пакета наклеивается силикатным клеем бумажная наклейка с оттиском печати «Для пакетов».

4.6. Отметка о количестве и адресатах размноженных экземпляров и копий документов с грифом «Для служебного пользования» вносится в журналы учета.

4.7. Ознакомление с документами с грифом «Для служебного пользования» осуществляется под подпись с указанием должности, фамилии муниципального служащего или работника структурного подразделения аппарата администрации города Южно-Сахалинска, отраслевого (функционального) органа, муниципального казенного и бюджетного учреждения, муниципального унитарного предприятия и даты ознакомления на последней странице документа.

4.8. Полномочное должностное лицо может давать разрешение на ознакомление с документами с грифом «Для служебного пользования» представителям сторонних организаций при наличии официального письменного мотивированного запроса организаций, которым такое право предоставлено действующим законодательством.

Запросы и все документы обоснований и разрешений на ознакомление с документами с пометкой «Для служебного пользования» приобщаются к соответствующему делу учета указанных документов.

4.9. Допускается изготовление выписок из документов с грифом «Для служебного пользования» и направление в другие структурные подразделения аппарата администрации города Южно-Сахалинска, отраслевые (функциональные) органы, муниципальные казенные и бюджетные учреждения, муниципальные унитарные предприятия, а также иные организации.

Выписка относится к служебным документам ограниченного распространения в случае, если в ней содержится информация, послужившая причиной установления пометки ограничения доступа. Должностное лицо, принявшее решение о подготовке выписки и включении в ее состав информации из служебного документа ограниченного распространения, несет персональную ответственность за обоснованность принятого решения. На оборотной стороне последнего листа документа с грифом «Для

служебного пользования» делается пометка «Выписка» и указывается перечень включенных в выписку страниц, разделов, пунктов и т.д. исходного документа, о количестве изготовленных выписок и где они учтены, заверяемые специалистом, осуществляющим регистрацию документа, с проставлением даты.

4.10. Направляемые для исполнения документы ограниченного распространения или их копии:

- передаются ответственными за ведение делопроизводства в структурных подразделениях аппарата администрации города Южно-Сахалинска, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий через лиц, допущенных к работе со служебными документами ограниченного распространения (с курьером), и от одного работника другому под личную подпись с отметкой в журнале учета;

- пересылаются сторонним организациям только специальной связью;

- не могут передаваться в электронном виде по незащищенным открытым каналам связи, международной сети Интернет, а также с использованием факсимильной связи.

V. Группировка исполненных документов ограниченного распространения в дела, отбор документов для хранения и к уничтожению

5.1. Документы с грифом «Для служебного пользования» после исполнения группируются в дела. При этом на обложке дела, в которое помещены такие документы, также проставляется гриф «Для служебного пользования». Порядок их группировки предусматривается номенклатурой дел несекретного делопроизводства. Порядок формирования дела осуществляется по правилам общего делопроизводства.

При небольшом количестве документов с пометкой «Для служебного пользования» номенклатурой дел может быть предусмотрено выделение одного дела: «Документы «Для служебного пользования».

5.2. Допускается помещать в дело «Документы «Для служебного пользования» отдельные не ограниченные к обороту документы, имеющие прямое отношение к содержанию документов данного дела.

5.3. Сброшюрованные материалы, издания, информационные материалы, планшеты и прочие материалы с грифом «Для служебного пользования», которые невозможно подшить в дела, хранятся отдельно. Одновременно заводится карточка учета выдачи дела, брошюры, издания (приложение № 5 к настоящей Инструкции), которая помещается в бумажный карман (конверт), приклеенный к внутренней стороне обложки, или хранится в специальном ящике - картотеке. Все карточки хранятся до уничтожения дела, брошюры, издания.

5.4. Проведение экспертизы научной и практической ценности документов и дел с грифом «Для служебного пользования» с целью отбора их на архивное хранение, установления сроков хранения, возможного снятия с них грифа «Для служебного пользования», рассмотрение и утверждение ее результатов производятся в соответствии с требованиями и порядком, установленными для служебных документов.

5.5. Отобранные к уничтожению документы и дела с грифом «Для служебного пользования», не имеющие исторической ценности и утратившие практическое значение, уничтожаются по отдельному акту или могут быть включены в один акт вместе с другими несекретными документами и делами.

После уничтожения материалов с грифом «Для служебного пользования» в учетных формах проставляется отметка:

«Уничтожено. Акт № ____ от __.__.____».
(дата)

Акты об уничтожении дел хранятся постоянно, а акты об уничтожении документов - 10 лет.

5.6. Допускается уничтожение не определенных в дела документов с проставлением отметок об уничтожении и даты уничтожения в графе «Отметка об уничтожении» журнала учета документов. Отметки об уничтожении заверяются подписями двух сотрудников соответствующего структурного подразделения аппарата администрации города Южно-Сахалинска, отраслевого (функционального) органа, муниципального казенного и бюджетного учреждения, муниципального унитарного предприятия.

5.7. Отобранные к уничтожению дела, документы и издания должны быть измельчены до степени, исключающей возможность прочтения текста.

VI. Порядок хранения документов, дел и изданий ограниченного распространения

6.1. Документы, дела и издания с грифом «Для служебного пользования», съемные машинные носители информации, содержащие информацию ограниченного распространения, должны храниться в служебных помещениях в надежно запираемых шкафах (сейфах, хранилищах).

6.2. Выданные для работы документы и дела с грифом «Для служебного пользования» с разрешения руководителя структурного подразделения аппарата администрации города Южно-Сахалинска, отраслевого (функционального) органа, муниципального казенного и бюджетного учреждения, муниципального унитарного предприятия могут находиться у исполнителя в течение срока, необходимого для выполнения

задания, при условии полного обеспечения их сохранности и соблюдения правил хранения.

6.3. Запрещается изъятие из дел или перемещение документов с грифом «Для служебного пользования» из одного дела в другое без разрешения лица, осуществляющего их учет. Обо всех проведенных изъятиях или перемещениях делаются отметки в журналах учета.

Запрещается выносить документы, дела и издания с грифом «Для служебного пользования» из служебных помещений для работы с ними на дому.

6.4. При смене в структурном подразделении аппарата администрации города Южно-Сахалинска, отраслевом (функциональном) органе, муниципальном казенном и бюджетном учреждении, муниципальном унитарном предприятии специалиста, отвечающего за учет и хранение документов, дел и изданий, съемных машинных носителей информации с грифом «Для служебного пользования», составляется акт приема-передачи этих документов, носителей информации, который утверждается руководителем структурного подразделения аппарата администрации города Южно-Сахалинска, отраслевого (функционального) органа, муниципального казенного и бюджетного учреждения, муниципального унитарного предприятия.

6.5. Проверка наличия документов, дел и изданий, съемных машинных носителей информации с грифом «Для служебного пользования» проводится не реже одного раза в год постоянно действующей технической комиссией по защите государственной тайны в администрации города Южно-Сахалинска. Результаты проверки оформляются актом.

6.6. В случае утраты документов, дел или изданий, съемных машинных носителей информации, содержащих служебную информацию ограниченного распространения, руководитель структурного подразделения аппарата администрации города Южно-Сахалинска, отраслевого (функционального) органа, муниципального казенного и бюджетного учреждения, муниципального унитарного предприятия, информирует об этом вице-мэра, руководителя аппарата администрации города Южно-Сахалинска и, совместно с сотрудниками отдела защиты информации Управления мобилизационной подготовки и защиты информации аппарата администрации города, проводит служебную проверку по факту утраты, о результатах которой докладывает вице-мэру, руководителю аппарата администрации города Южно-Сахалинска.

На безвозвратно утраченные документы, дела и издания, съемные машинные носители информации с грифом «Для служебного пользования» составляется акт, на основании которого делаются соответствующие отметки в учетных формах.

Акты на утраченные дела постоянного срока хранения после их утверждения передаются в Архивный отдел аппарат администрации города для включения в дело фонда.

VII. Порядок снятия грифа «Для служебного пользования» с носителей информации ограниченного распространения

7.1. Снятие грифа «Для служебного пользования» с носителей информации ограниченного распространения осуществляется:

- по решению должностного лица, подписавшего или утвердившего документ, либо вышестоящего по должности руководителя;
- по решению экспертной комиссии администрации города Южно-Сахалинска, оформленному в виде акта при проведении экспертизы ценности документов.

Снятие с документов ограниченного распространения грифа «Для служебного пользования» осуществляется путем зачеркивания на подлиннике документа указанной пометки с проставлением отметки со ссылкой на акт, его номер и дату или указания должности, фамилии и инициалов должностного лица, снявшего ограничение, его подписи и даты.

7.2. О снятии грифа «Для служебного пользования» с носителей информации ограниченного распространения в регистрационно-учетных формах делаются соответствующие записи, о чем уведомляются все адресаты, которым эти документы направлялись.

VIII. Требования, предъявляемые к автоматизированной обработке служебной информации ограниченного распространения

8.1. Автоматизированная обработка служебной информации ограниченного распространения допускается только на автономных персональных электронно-вычислительных машинах (ПЭВМ) или в локальных вычислительных сетях (далее - ЛВС) структурных подразделений Правительства области, расположенных в пределах контролируемой зоны, в которой расположено структурное подразделение аппарата администрации города Южно-Сахалинска, отраслевой (функциональный) орган, муниципальное казенное и бюджетное учреждение, муниципальное унитарное предприятие. Допускается подключение ПЭВМ или ЛВС к другой автоматизированной системе или единой мультисервисной телекоммуникационной сети администрации города Южно-Сахалинска (ЕМТС) при соблюдении установленных Федеральной службой по техническому и экспортному контролю требований по организации технической защиты информации, не составляющей государственную тайну.

8.2. Уровень технической защиты информации, а также перечень необходимых организационных и технических решений, определяется по заявке руководителя структурного подразделения аппарата администрации города Южно-Сахалинска, отраслевого (функционального) органа, муниципального казенного и бюджетного учреждения, муниципального унитарного предприятия, по результатам обследования объекта защиты (ПЭВМ или ЛВС) специалистами отдела защиты информации Управления мобилизационной подготовки и защиты информации администрации города и Управления информатизации муниципального казенного учреждения «Управление делами администрации города Южно-Сахалинска».

8.3. Все работы, связанные с автоматизированной обработкой служебной информации ограниченного распространения, производятся только с использованием учтенных машинных носителей информации (МНИ).

Учет МНИ осуществляют муниципальные служащие и работники структурных подразделений аппарата администрации города Южно-Сахалинска, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий, ответственные за учет служебных документов ограниченного распространения, или специалисты, ответственные за выдачу и установку МНИ.

К МНИ относятся:

- несъемные жесткие магнитные диски;
- съемные жесткие магнитные диски;
- гибкие магнитные диски;
- оптические и магнитооптические диски;
- флэш-накопители.

МНИ, используемые для обработки информации ограниченного распространения, должны быть учтены в журналах установленной формы (приложение № 5 к настоящей Инструкции). При небольшом их количестве допускается учитывать в журнале учета документов «Для служебного пользования».

8.4. На съемных МНИ ограниченного распространения любым доступным способом проставляются учетные реквизиты: учетный номер с пометкой «ДСП», номер экземпляра, подпись ответственного за учет работника, а также другие возможные реквизиты, идентифицирующие этот носитель.

8.5. МНИ ограниченного распространения, непригодные для дальнейшего использования, уничтожаются ответственным за учет документов ограниченного распространения совместно со специалистом отдела защиты информации Управления мобилизационной подготовки и защиты информации администрации города путем их физического разрушения (разрушение рабочей поверхности носителя любым возможным

способом) с отражением факта уничтожения в журнале учета МНИ. Перед уничтожением МНИ ограниченного распространения с него должна быть стерта (уничтожена) информация, если это позволяют физические принципы работы носителя.

Начальник Управления мобилизационной
подготовки и защиты информации

В.В.Кочкин

Приложение № 1
к инструкции о порядке обращения со служебной
информацией ограниченного распространения
в администрации города Южно-Сахалинска

ЖУРНАЛ
учета документов с грифом «Для служебного пользования»

1-я страница

Дата поступления и индекс документа	Дата и индекс документа	Откуда поступил или куда направлен	Вид носителя, наименование документа и краткое содержание	Количество листов		Номера экземпляров
				документа	приложения	
1	2	3	4	5	6	7

2-я страница

Резолюция или кому направлен на исполнение	Отметка о постановке на контроль и срок исполнения	Дата и расписка		Индекс (номер) дела, куда подшит документ	Отметки об уничтожении, дата, подпись	Примечание
		в получении	о возврате			
8	9	10	11	12	13	14

Приложение № 2
к инструкции о порядке обращения со служебной
информацией ограниченного распространения
в администрации города Южно-Сахалинска

ОБРАЗЕЦ
оформления списка рассылки размноженных документов
с грифом «Для служебного пользования»

Список рассылки к исх. № - / дсп от . .20

№ экз.	Адресат
1.	В дело
2.	Управление внутренней политики
3.	Департамент экономического развития
4.	Управление административно-политической деятельности
5.	Отдел по делам несовершеннолетних и защите их прав
6.	Отдел социальных выплат
7.	Департамент продовольственных ресурсов и потребительского рынка
8.	Департамент правового обеспечения
9.	Отдел муниципального жилищного контроля
10.	Отдел контроля в сфере закупок
11.	Управление охраны окружающей среды
12.	Управление кадровой политики
13.	Финансовое управление
14.	Департамент по управлению муниципальным имуществом
15.	Департамент архитектуры, градостроительства и землепользования
16.	Департамент городского хозяйства
17.	Управление культуры
18.	Управление по физической культуре и спорту
19.	Департамент образования
20.	МКУ «Управление по делам ГО и ЧС города Южно-Сахалинска»
21.	МКУ «Управление делами администрации города Южно-Сахалинска»

Всего 21 экземпляр

Руководитель структурного подразделения
аппарата администрации города
(отраслевого (функционального)
органа, МКУ, МБУ или МУП)

(Ф.И.О.)

Приложение № 3
к инструкции о порядке обращения со служебной
информацией ограниченного распространения
в администрации города Южно-Сахалинска

ОБРАЗЕЦ
оформления списка рассылки копий документов
с грифом «Для служебного пользования»

Список рассылки к исх. N ____ - ____ / ____ дсп от ____ . ____ .20 ____ г.

№ экз.	Адресат	Вх. (рег.) № ____ - ____ / ____ дсп от ____ . ____ .20 экз. №
1.	В дело	-
2.	Управление внутренней политики	копия № 1
3.	Департамент экономического развития	копия № 2
4.	Управление административно-политической деятельности	копия № 3
5.	Отдел по делам несовершеннолетних и защите их прав	копия № 4
6.	Отдел социальных выплат	копия № 5
7.	Департамент продовольственных ресурсов и потребительского рынка	копия № 6
8.	Департамент правового обеспечения	копия № 7
9.	Отдел муниципального жилищного контроля	копия № 8
10.	Управление кадровой политики	копия № 9
11.	Управление охраны окружающей среды	копия № 10
12.	Департамент по управлению муниципальным имуществом	копия № 11

Всего 11 копий

Руководитель структурного подразделения
аппарата администрации города
(отраслевого (функционального)
органа, МКУ, МБУ или МУП)

(Ф.И.О.)

Приложение № 5
к инструкции о порядке обращения со служебной
информацией ограниченного распространения
в администрации города Южно-Сахалинска

ЖУРНАЛ
учета машинных носителей информации
с грифом «Для служебного пользования»

1-я страница

Учетный номер и ограничительная пометка МНИ, дата регистрации	Входящий/ исходящий номер, ограничительная пометка МНИ, дата	Тип и марка МНИ, краткое содержание	Откуда поступил или куда направлен	Кому выдан МНИ (подразделение, Ф.И.О.)
1	2	3	4	5

2-я страница

Место нахождения/ хранения МНИ (адрес, кабинет, ПЭВМ)	Дата и расписка		Отметка об уничтожении/ форматировании МНИ (дата, подпись)	Примечание
	в получении	о возврате		
6	7	8	9	10

УТВЕРЖДЕНО

постановлением администрации
города Южно-Сахалинска
от 26.05.2014 № 903-па

**ПОЛОЖЕНИЕ
ОБ ОРГАНИЗАЦИИ ЗАЩИТЫ СЛУЖЕБНОЙ ИНФОРМАЦИИ
ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ В АДМИНИСТРАЦИИ
ГОРОДА ЮЖНО-САХАЛИНСКА**

1. Общие положения

1.1. Настоящее Положение о порядке организации и проведения работ по защите служебной информации ограниченного распространения в администрации города Южно-Сахалинска (далее - Положение) разработано на основании требований 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 г. № 912-51, Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Специальных требований и рекомендаций по технической защите конфиденциальной информации, утвержденных Приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

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

1.3. Термины и понятия, используемые в настоящем Положении:

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информация, требующая защиты, - сведения об администрации города Южно-Сахалинска (далее - администрация города) и ее деятельности, на распространение которых накладываются ограничения действующим законодательством Российской Федерации, нормативными правовыми актами Сахалинской области и города Южно-Сахалинска.

Защита информации от несанкционированного доступа - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными правовыми актами или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с

заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Система защиты информации - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

1.4. Цель данного Положения - на основании действующих нормативных правовых актов и руководящих документов по защите информации создать необходимые организационно-правовые основы для эффективной защиты служебной информации ограниченного распространения.

1.5. Положение определяет порядок организации в администрации города работ по разработке и эксплуатации объектов информатизации и систем защиты информации (далее - СЗИ).

1.6. Положение предназначено для практического использования лицами, ответственными за защиту информации в администрации города.

1.7. Требования настоящего Положения являются обязательными для исполнения всеми муниципальными служащими и работниками во всех структурных подразделениях аппарата администрации города, отраслевых (функциональных) органах, муниципальных казенных и бюджетных учреждениях, муниципальных унитарных предприятиях.

1.8. Ответственность за общее состояние защиты служебной информации ограниченного распространения возлагается на вице-мэра, руководителя аппарата администрации города.

Ответственность за организацию мероприятий по защите информации в структурных подразделениях аппарата администрации города, отраслевых (функциональных) органах, муниципальных казенных и бюджетных учреждениях, муниципальных унитарных предприятиях, возлагается на начальника отдела защиты информации Управления мобилизационной подготовки и защиты информации аппарата администрации города.

Ответственность за проведение мероприятий по технической защите информации в структурных подразделениях аппарата администрации города, отраслевых (функциональных) органах, муниципальных казенных и бюджетных учреждениях, муниципальных унитарных предприятиях возлагается на начальника Управления информатизации МКУ «Управление делами администрации города Южно-Сахалинска».

Контроль выполнения требований настоящего Положения возлагается на вице-мэра, руководителя аппарата администрации города.

1.9. Для оказания услуг в области защиты информации могут привлекаться специализированные организации, имеющие лицензию на этот вид деятельности.

1.10. Используемые технические и программные средства защиты информации должны быть сертифицированы в соответствии с требованиями Положения о сертификации средств защиты информации, утвержденного Постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

2. Охраняемые сведения и потенциальные угрозы

2.1. Результатом защиты информации является предотвращение ущерба из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Целями технической защиты служебной информации ограниченного доступа в администрации города являются:

- предотвращение утечки охраняемых сведений по техническим каналам;

- предотвращение несанкционированного доступа (далее - НСД) к информации, ее разрушения, искажения, уничтожения, блокировки и несанкционированного копирования в системах и средствах автоматизации.

2.2. Замысел достижения целей защиты информации.

Замыслом достижения целей защиты информации является обеспечение защиты информации путем строгого соблюдения действующих норм и требований ФСТЭК России (Гостехкомиссии России), созданием СЗИ объектов информатизации и принятием эффективных режимных мер, предписанных руководящими документами.

2.3. Охраняемые сведения:

- служебная информация ограниченного распространения, обрабатываемая с использованием технических средств;

- служебная информация ограниченного распространения, содержащаяся в речевой информации.

2.4. Потенциальные угрозы информационной безопасности объектов.

В качестве угроз информационной безопасности объектов необходимо рассматривать:

- использование разведками иностранных государств технических средств для получения охраняемых сведений, перехват информации, обсуждаемой в защищаемых помещениях и циркулирующей в основных технических средствах и системах, а также воздействие на информационные ресурсы автоматизированных систем с целью разрушения, искажения и блокирования информации;

- использование криминальными структурами технических средств для получения информации, представляющей ценность в интересах планирования криминальных акций;

- несанкционированный удаленный доступ (из-за пределов контролируемых зон) в сети систем информатизации и связи объектов с целью получения служебной информации ограниченного доступа и использования возможностей систем связи (компьютерная разведка, дистанционный доступ к программным средствам иностранных цифровых электронных автоматических телефонных станций);

- преднамеренные действия нарушителей и злоумышленников, незаконным путем проникших на объекты посредством контактного несанкционированного доступа к элементам автоматизированных систем, к носителям информации, к вводимой и выводимой информации, к программному обеспечению, а также подключения к линиям связи;

- непреднамеренные действия сотрудников администрации города, приводящие к утечке, искажению, разрушению информации, подлежащей защите, в том числе ошибки проектирования, разработки и эксплуатации технических и программных средств автоматизированных систем.

2.5. Оценка возможностей технических средств разведки иностранных государств и криминальных структур проводится с использованием модели иностранной технической разведки, методик оценки возможностей иностранной технической разведки и других нормативных документов ФСТЭК России (Гостехкомиссии России) применительно к охраняемым сведениям об объектах, к информации, циркулирующей (обсуждаемой) в защищаемых помещениях и основных технических средствах и системах объектов.

2.6. Для ведения перехвата информации, циркулирующей в средствах и системах информатизации и связи объектов в администрации города, могут использоваться следующие виды технической разведки:

- стационарная;
- портативная возимая;
- портативная носимая;
- автономная автоматическая.

2.7. Одной из возможных угроз информационным ресурсам автоматизированных систем при определенных условиях может являться компьютерная разведка, направленная на извлечение, систематизацию и специальную обработку открытой информации из информационно-вычислительных сетей, телекоммуникационных систем, а также информации об особенностях их построения и функционирования. Таким условием может быть несанкционированный выход с отдельных рабочих мест автоматизированных систем в глобальные информационные сети. Бесконтрольное подключение к информационно-вычислительным сетям общего пользования компьютерных средств и оргтехники, находящихся на

защищаемых объектах, может служить предпосылкой к утечке охраняемой информации.

3. Порядок ввода в эксплуатацию объектов информатизации

3.1. Организационно-техническими мероприятиями, необходимыми для ввода в эксплуатацию средств вычислительной техники, на которых происходит обработка служебной информации ограниченного доступа, а также автоматизированных систем обработки служебной информации ограниченного доступа, являются:

- классификация средств вычислительной техники и автоматизированных систем по защите информации от несанкционированного доступа;

- определение специальных требований (требования по электропитанию, заземлению, размещению, по использованию средств защиты информации от несанкционированного доступа и от ее утечки по техническим каналам и др.);

- проверка выполнения специальных требований по защите служебной информации ограниченного распространения на месте эксплуатации средств вычислительной техники или автоматизированных систем;

- определение состава и содержания необходимых защитных мероприятий на основании сформулированных специальных требований по защите информации на месте эксплуатации средств вычислительной техники или автоматизированных систем;

- издание распоряжений администрации города о вводе в эксплуатацию либо о разрешении на эксплуатацию средств вычислительной техники и автоматизированных систем, на которых производится обработка служебной информации ограниченного доступа;

- разработка организационно-распорядительной документации (инструкции по эксплуатации технических и программных средств защиты от НСД, журналы установленной формы по учету накопителей информации, о назначении лиц, ответственных за эксплуатацию, акты классификации АС, технические паспорта на АС и др.);

- проведение периодического контроля эффективности принятых мер защиты.

3.2. Классификация средств вычислительной техники и автоматизированных систем по защите информации от несанкционированного доступа.

3.2.1. В целях дифференцированного подхода к защите служебной информации ограниченного распространения, обрабатываемой в администрации города, проводится классификация средств вычислительной

техники и автоматизированных систем по защите информации от несанкционированного доступа.

3.2.2. Классификации подлежат все действующие, но ранее не классифицированные средства вычислительной техники и автоматизированные системы, предназначенные для обработки служебной информации ограниченного распространения.

3.2.3. Выбор класса автоматизированной системы осуществляется в соответствии с рекомендациями руководящего документа ФСТЭК России «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации».

4. Организационные и технические мероприятия по защите служебной информации ограниченного распространения

4.1. Защита служебной информации ограниченного распространения в администрации города достигается путем создания системы защиты информации, которая включает комплекс организационных, технических и программных мероприятий, направленных на закрытие технических каналов утечки информации.

4.2. Мероприятия по защите информации являются составной частью деятельности администрации города, проводятся с целью закрытия возможных технических каналов утечки информации. Эти мероприятия проводятся на всех циклах создания, развития и эксплуатации используемых технических систем и средств, а также при ремонте, реконструкции и эксплуатации защищаемых помещений.

4.3. С целью закрытия возможных технических каналов утечки речевой конфиденциальной информации в администрации города необходимо проведение следующих организационно-режимных мероприятий:

- закрытие дверей в защищаемые помещения между мероприятиями и в нерабочее время на ключ;

- установка и замена средств вычислительной техники только по согласованию и под контролем сотрудников отдела защиты информации Управления мобилизационной подготовки и защиты информации аппарата администрации города и Управления информатизации МКУ «Управление делами администрации города Южно-Сахалинска».

4.4. С целью закрытия возможных каналов утечки сведений, отнесенных к служебной информации ограниченного распространения, при их обработке и хранении в автоматизированных системах и на средствах вычислительной техники необходимо применение следующих мер защиты:

- использование сертифицированных средств защиты информации;

- издание правовых актов, регулирующих вопросы сбора, обработки, хранения, защиты, передачи служебной информации ограниченного распространения, а также вопросы ответственности за ее разглашение;

- выполнение положений Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных Приказом Гостехкомиссии России от 30 августа 2002 г. № 282, Приказов ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и 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», при организации обработки информации в локальных вычислительных сетях;

- выполнение требований Указа Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

- организация процесса резервного копирования и архивирования как неотъемлемой части политики защиты информации.

4.5. Документальное оформление мероприятий по защите информации включает:

- издание распоряжения об утверждении перечня защищаемых объектов вычислительной техники, предназначенных для обработки служебной информации ограниченного распространения;

- издание распоряжений о вводе в эксплуатацию либо о разрешении на эксплуатацию средств вычислительной техники и автоматизированных систем, на которых производится обработка служебной информации ограниченного распространения;

- утверждение актов классификации автоматизированных систем по требованиям защиты от несанкционированного доступа к информации;

- утверждение и поддержание в актуальном состоянии паспортов защищаемых средств вычислительной техники.

5. Обязанности и права должностных лиц

5.1. Вице-мэр, руководитель аппарата администрации города:

- контролирует выполнение требований настоящего Положения;
- отвечает за общее состояние технической защиты служебной информации ограниченного распространения в администрации города;

- утверждает перечень защищаемых основных технических систем и средств, также другие документы по вопросам защиты информации;

- утверждает акты классификации средств вычислительной техники и автоматизированных систем;

- участвует в определении помещений, в которых необходимо проводить мероприятия с обсуждением вопросов конфиденциального характера (защищаемые помещения), мест установки и количества СВТ, необходимых для обработки информации, требующей защиты.

5.2. Начальник отдела защиты информации Управления мобилизационной подготовки и защиты информации аппарата администрации города:

- осуществляет организацию и координацию работ по защите информации в соответствии с руководящими документами по данному вопросу;

- совместно с руководителями структурных подразделений аппарата администрации города, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий, осуществляет планирование мероприятий по защите информации, мероприятий по подготовке объектов информатизации к работе со служебной информацией ограниченного распространения, организует их выполнение и контроль эффективности принятых мер;

- разрабатывает организационно-распорядительные документы по вопросам защиты информации;

- анализирует информацию, циркулирующую в средствах вычислительной техники, а также автоматизированных системах, состояние защищенности информационных ресурсов, определяет возможные технические каналы утечки, готовит предложения по совершенствованию системы защиты, систематизирует и распространяет положительный опыт работы;

- определяет возможности перехвата информации техническими средствами разведки, несанкционированного доступа к ней, разрушения (уничтожения) и искажения, разрабатывает соответствующие меры по ее защите;

- участвует в рассмотрении и согласовании документов, определяющих пропускной и внутриобъектовый режим, разрабатывает предложения по финансированию мероприятий, связанных с защитой информации;

- принимает меры по предупреждению, выявлению и пресечению попыток неправомерного доступа к служебной информации ограниченного распространения или попыток их хищения, копирования, изменения, докладывает соответствующим руководителям об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации;

- координирует работы по защите информации, проводимые в структурных подразделениях аппарата администрации города, отраслевых (функциональных) органах, муниципальных казенных и бюджетных

учреждениях, муниципальных унитарных предприятиях, оказывает им практическую и методическую помощь;

- организует контроль состояния системы защиты информации, выполнения требований законодательства Российской Федерации по вопросам защиты информации, нормативных документов ФСТЭК России (Гостехкомиссии России);

- исполняет необходимую отчетную документацию о состоянии работ по защите информации, разрабатывает предложения по дальнейшему совершенствованию системы защиты информации при использовании технических средств в соответствии с Планом работы администрации города по вопросам информационной безопасности на соответствующий календарный год.

Начальник отдела защиты информации Управления мобилизационной подготовки и защиты информации аппарата администрации города района имеет право:

- контролировать исполнение требований вышестоящих организаций и нормативных правовых актов администрации города по вопросам сохранения конфиденциальной информации;

- требовать от руководителей проверяемых подразделений устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;

- требовать от работников представления письменных объяснений по фактам нарушения ими режима защиты служебной информации ограниченного распространения;

- готовить проекты контрактов на выполнение работ по защите информации со сторонними организациями, имеющими необходимые лицензии;

- вносить предложения по совершенствованию системы защиты информации, изменению категорий объектов информатизации, степени конфиденциальности обрабатываемой информации.

5.3. Начальник Управления информатизации МКУ «Управление делами администрации города Южно-Сахалинска» :

- обеспечивает техническую защиту информации, циркулирующей в автоматизированных системах, в том числе передаваемой по каналам связи, организует во взаимодействии с отделом защиты информации Управления мобилизационной подготовки и защиты информации аппарата администрации города работы по проведению специальных исследований технических средств обработки и передачи информации, по аттестации объектов вычислительной техники на соответствие нормативным требованиям, в т.ч. с привлечением специализированных организаций, имеющих лицензию на проведение такого рода работ;

- проводит систематический контроль работы средств технической защиты информации, применяемых на объектах вычислительной техники, а также следит за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;

- обобщает и анализирует сведения о противоправных устремлениях к информации, попытках преодоления систем технической защиты информации, используемых при этом методах и средствах;

- анализирует состояние защищенности информационных ресурсов сети, готовит предложения по совершенствованию систем технической защиты, систематизирует и распространяет положительный опыт работы;

- участвует в проведении обследования структурных подразделений аппарата администрации города, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий, с целью выявления служебной информации ограниченного распространения, циркулирующей в средствах вычислительной техники, а также с целью выявления существующих угроз безопасности информации, определяет практические мероприятия по устранению имеющихся недостатков;

- принимает меры по предупреждению угроз безопасности информации, возникающих в результате случайных ошибок персонала при обработке электронных документов, с учетом специфики конкретного места обработки и применяемых средств защиты;

- принимает участие в оценке реальной опасности утечки информации, подлежащей защите при использовании технических средств, в разработке эффективных и экономически обоснованных мер по ее защите;

- организует работу по эксплуатации системы технической защиты информации в автоматизированных системах обработки электронных документов;

- проводит работы по внедрению технических и программных средств защиты информации от несанкционированного доступа к ней на действующих автоматизированных системах и отдельных средствах вычислительной техники;

- обеспечивает эксплуатацию технических и программных средств защиты информации на действующих автоматизированных системах и отдельных средствах вычислительной техники, контролирует работоспособность и эффективность функционирования этих средств;

- распределяет между пользователями средств вычислительной техники необходимые реквизиты криптографической защиты (пароли, ключи защиты и т.п.), формирует и распределяет между пользователями необходимые реквизиты защиты от несанкционированного доступа (в зависимости от системы защиты);

- проводит контроль целостности технических средств защиты информации, программного обеспечения с целью выявления несанкционированных изменений в них;

- контролирует проведение пользователями резервного копирования (архивирования) служебной информации ограниченного распространения, соблюдение мер специальной защиты при эксплуатации средств вычислительной техники;

- принимает участие в разработке документов по обеспечению безопасности информации при эксплуатации единой мультисервисной телекоммуникационной сети администрации города;

- не допускает подключения к единой мультисервисной телекоммуникационной сети администрации города или к средствам вычислительной техники нештатных блоков и устройств, не имеющих разрешения на эксплуатацию;

- проводит периодический контроль средств вычислительной техники, подключенных к единой мультисервисной телекоммуникационной сети, на предмет исключения несанкционированного изменения в составе, конструкции, конфигурации, размещении средств вычислительной техники, а также в составе программного обеспечения;

- осуществляет контроль прав доступа пользователей к информационным ресурсам единой мультисервисной телекоммуникационной сети;

- осуществляет контроль разграничения прав доступа к защищаемой информации на несъемных носителях информации рабочих мест пользователей;

- регулярно анализирует содержимое системных журналов, проводит работы по выявлению возможных каналов утечки служебной информации ограниченного распространения за счет несанкционированных доступов к информации и техническим средствам вычислительной техники, ведет их учет;

- ведет аудит единой мультисервисной телекоммуникационной сети;

- осуществляет контроль соблюдения требований по безопасности информации при использовании машинных носителей информации;

- разрабатывает и вводит установленным порядком необходимую учетную и объектовую документацию (журнал учета идентификаторов, инструкции пользователям и т.д.);

- принимает меры по предупреждению, выявлению и пресечению попыток неправомерного доступа к служебной информации ограниченного распространения или попыток их хищения, копирования, изменения, сообщает начальнику отдела защиты информации Управления мобилизационной подготовки и защиты информации аппарата администрации города об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации.

Начальник Управления информатизации МКУ «Управление делами администрации города Южно-Сахалинска», имеет право:

- иметь доступ к средствам обработки и передачи информации подразделений, постоянно осуществлять проверки состояния защиты информации, контролировать состояние защищенности объектов информатизации;

- требовать от пользователей автоматизированных систем безусловного соблюдения установленной технологии обработки электронных документов и выполнения требований по информационной безопасности.

5.4. Пользователи средств вычислительной техники предназначенных для обработки служебной информации ограниченного распространения обязаны:

- строго соблюдать меры по защите информации и правила эксплуатации средств вычислительной техники, установленные нормативными правовыми актами администрации города;

- обеспечивать сохранность комплекта ПЭВМ, машинных носителей информации и целостность установленного программного обеспечения;

- знать и соблюдать установленные требования по учету, хранению и пересылке машинных, бумажных и иных носителей информации;

- применять антивирусные программы при включении средств вычислительной техники или при использовании внешних носителей информации;

- по окончании обработки служебной информации ограниченного распространения «обнулить» оперативную память компьютера путем его перезагрузки или временного выключения.

5.5. Руководители структурных подразделений аппарата администрации города, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий :

- организуют выполнение мероприятий по защите служебной информации ограниченного распространения при использовании технических средств;

- участвуют в определении правил разграничения доступа к информации в системах и средствах информатизации, используемых в администрации города;

- согласовывают с начальником Управления информатизации МКУ «Управление делами администрации города Южно-Сахалинска» установку, замену и перемещение технических средств в помещениях, где обрабатывается служебная информация ограниченного распространения.

6. Планирование работ по защите служебной информации ограниченного распространения

6.1. Планирование работ по защите информации проводится на основании:

- рекомендаций актов проверок контрольными органами ФСТЭК России;
- результатов анализа деятельности в области защиты информации;
- рекомендаций и указаний ФСТЭК России;
- решений Постоянно действующей технической комиссии по защите государственной тайны в администрации города Южно-Сахалинска;
- рекомендаций совета по защите информации при Правительстве Сахалинской области.

6.2. Для подготовки и реализации организационных и технических мероприятий по защите информации, а также для увязки этих мероприятий с планами работ структурных подразделений аппарата администрации города, отраслевых (функциональных) органов, муниципальных казенных и бюджетных учреждений, муниципальных унитарных предприятий, составляется годовой план работ по защите информации.

6.3. Годовой план работ по защите информации разрабатывается начальником отдела защиты информации Управления мобилизационной подготовки и защиты информации аппарата администрации города совместно с начальником Управления информатизации МКУ «Управления делами администрации города Южно-Сахалинска» и утверждается вице-мэром, руководителем аппарата администрации города.

В годовом плане указываются:

- планируемые работы по защите информации и контролю ее эффективности;
- структурные подразделения аппарата администрации города, отраслевые (функциональные) органы, муниципальные казенные и бюджетные учреждения, муниципальные унитарные предприятия, должностные лица, отвечающие за выполнение указанных работ, и исполнители этих работ;
- сроки выполнения работ.

6.4. Контроль выполнения годового плана возлагается на вице-мэра, руководителя аппарата администрации города.

7. Контроль состояния защиты служебной информации ограниченного доступа

7.1. С целью своевременного выявления и предотвращения утечки служебной информации ограниченного распространения по техническим

каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность систем информатизации, осуществляется контроль состояния и эффективности защиты информации.

7.2. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

7.3. Повседневный контроль выполнения организационных и технических мероприятий, направленных на обеспечение защиты информации, проводится начальником отдела защиты информации Управления мобилизационной подготовки и защиты информации аппарата администрации города совместно с начальником Управления информатизации МКУ «Управления делами администрации города Южно-Сахалинска».

7.4. Периодический контроль может осуществляться представителями ФСТЭК России, территориальных органов ФСБ России, совета по защите информации при Правительстве Сахалинской области.

7.5. Допуск представителей этих органов для проведения контроля состояния защиты информации осуществляется в установленном порядке по предъявлении служебных удостоверений и предписаний на право проверки, подписанных руководителем (заместителем) соответствующего органа.

7.6. К контролю эффективности мероприятий по защите информации могут привлекаться специалисты проверяемых подразделений.

7.7. Результаты проверок отражаются в техническом паспорте объекта информатизации.

7.8. Периодичность проверок объектов информатизации, где обрабатывается (обсуждается) конфиденциальная информация, не реже 1 раза в год и при каждом изменении состава и расположения основных технических средств и систем.

7.9. Начальник отдела защиты информации Управления мобилизационной подготовки и защиты информации аппарата администрации города либо лицо, его замещающее, обязан присутствовать при всех проверках администрации города по вопросам защиты информации.

7.10. По результатам проверок контролирующими органами начальник отдела защиты информации Управления мобилизационной подготовки и защиты информации аппарата администрации города совместно с начальником Управления информатизации МКУ «Управления делами администрации города Южно-Сахалинска», с привлечением других заинтересованных специалистов в месячный срок разрабатывает план устранения выявленных недостатков.

7.11. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

7.12. При обнаружении нарушений вице-мэр, руководитель аппарата администрации города обязан принять все необходимые меры по их устранению в сроки, согласованные с органом или лицом, проводившим проверку.

Начальник Управления мобилизационной
подготовки и защиты информации

В.В.Кочкин