



**Управление по государственному регулированию цен (тарифов)
Ненецкого автономного округа**

ПРИКАЗ

от 26 июня 2017 г. № 11
г. Нарьян-Мар

**О порядке обращения со служебной информацией
ограниченного доступа в Управлении
по государственному регулированию цен (тарифов)
Ненецкого автономного округа**

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденным постановлением Правительства Российской Федерации от 03.11.1994 № 1233, Положением об Управлении по государственному регулированию цен (тарифов) Ненецкого автономного округа, утвержденным постановлением Администрации Ненецкого автономного округа от 17.08.2012 № 233-п, в целях установления единых требований к обращению со служебной информацией ограниченного доступа в Управлении по государственному регулированию цен (тарифов) Ненецкого автономного округа ПРИКАЗЫВАЮ:

1. Утвердить:

1) Положение о порядке обращения со служебной информацией ограниченного доступа в Управлении по государственному регулированию цен (тарифов) Ненецкого автономного округа согласно Приложению 1 к настоящему приказу;

2) Инструкцию по обработке информации ограниченного доступа с использованием средств вычислительной техники в Управлении по государственному регулированию цен (тарифов) Ненецкого автономного округа согласно Приложению 2 к настоящему приказу;

3) Примерный перечень служебной информации ограниченного доступа в Управлении по государственному регулированию цен (тарифов) Ненецкого автономного округа согласно Приложению 3 к настоящему приказу.

2. Настоящий приказ вступает в силу со дня официального опубликования.

Исполняющий обязанности
начальника Управления



Л.В. Тихомирова

Приложение 1
к приказу Управления по
государственному регулированию
цен (тарифов)
Ненецкого автономного округа
от 26.06.2017 № 11
«О порядке обращения со служебной
информацией ограниченного доступа
в Управлении по государственному
регулированию цен (тарифов)
Ненецкого автономного округа»

**Положение
о порядке обращения со служебной информацией
ограниченного доступа в Управлении по государственному
регулированию цен (тарифов) Ненецкого автономного округа**

**Раздел I
Общие положения**

1. Настоящее Положение, разработанное в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных») и Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон «Об информации, информационных технологиях и о защите информации»), определяет общий порядок обращения с документами на различных носителях, в том числе с электронными документами и сообщениями, содержащими служебную информацию ограниченного доступа, не отнесенную к сведениям, составляющим государственную тайну (далее – служебная информация ограниченного доступа), в Управлении по государственному регулированию цен (тарифов) Ненецкого автономного округа (далее – Управление).

2. К служебной информации ограниченного доступа в Управлении относится служебная информация, не отнесенная к сведениям, составляющим государственную тайну, используемая в повседневной деятельности Управления, к которой нет свободного доступа на основании требований федеральных законов, обладающая действительной или потенциальной ценностью в силу ее неизвестности лицам, не имеющим права доступа к ней, и по отношению к которой в Управлении принимаются правовые, организационные, технические и иные меры защиты информации.

3. Примерный перечень сведений, которые относятся к служебной информации ограниченного доступа в Управлении (далее – Примерный перечень сведений), утверждается приказом Управления.

Сведения, не включенные в Примерный перечень сведений, могут быть отнесены к служебной информации ограниченного доступа в случае, если это не

противоречит требованиям законодательства Российской Федерации и не нарушает права граждан на доступ к информации.

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

акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;

решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;

сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

5. В настоящем Положении используются следующие основные понятия:

носители сведений, содержащих служебную информацию ограниченного доступа (носители служебной информации ограниченного доступа) – материальные объекты, в том числе физические поля, в которых информация ограниченного доступа находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

съёмный машинный носитель информации – сменный носитель данных, предназначенный для записи и считывания данных, представленных в стандартных кодах (гибкие магнитные диски, оптические (лазерные) компакт-диски, внешние жесткие диски, USB-флеш-накопители, магнитные ленты и др.);

учетные формы – книги, журналы, реестры и карточки учета (регистрации) документов, которые ведутся в делопроизводстве, а также компьютерные программно-технические средства и системы электронного учета документооборота;

техническая защита информации – защита (не криптографическими методами) служебной информации ограниченного доступа от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования;

контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств;

средство защиты информации – техническое, программное средство, предназначенное (используемое) для защиты служебной информации ограниченного доступа;

средство вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Иные понятия, используемые в настоящем Положении, применяются в значениях, определенных Федеральным законом «О персональных данных» и Федеральным законом «Об информации, информационных технологиях и о защите информации».

6. Ответственность за организацию порядка обращения со служебной информацией ограниченного доступа в Управлении возлагается на начальника Управления.

7. В Управлении назначаются государственные гражданские служащие, ответственные за соблюдение порядка обращения со служебной информацией ограниченного доступа.

8. Техническую защиту служебной информации ограниченного доступа в Управлении обеспечивает казенное учреждение Ненецкого автономного округа «Ненецкий информационно-аналитический центр».

9. Для оказания услуг в области защиты служебной информации ограниченного доступа Управлением могут привлекаться юридические лица и индивидуальные предприниматели, имеющие лицензии на этот вид деятельности в случаях, предусмотренных Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

10. В случае изменения структуры Управления решение о дальнейшем использовании носителей служебной информации ограниченного доступа, имеющихся в структурных подразделениях Управления, принимает комиссия, создаваемая распоряжением Управления.

Раздел II

Техническая защита служебной информации ограниченного доступа

11. Техническая защита служебной информации ограниченного доступа в Управлении осуществляется в соответствии с законодательством Российской Федерации, стандартами и иными правовыми актами Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) в области защиты информации, а также настоящим Положением.

12. Создание систем защиты персональных данных, обрабатываемых в информационных системах персональных данных Управления, осуществляется в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (далее – Требования к защите персональных данных), Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18.02.2013 № 21.

Обеспечение безопасности персональных данных при их обработке в государственных информационных системах Управления (далее – ГИС) осуществляется в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в ГИС, утвержденными

приказом ФСТЭК России от 11.02.2013 № 17 (далее – Требования о защите информации) и Требованиями к защите персональных данных.

При обработке персональных данных в ГИС должно быть обеспечено соответствующее соотношение класса защищенности ГИС с уровнем защищенности персональных данных в соответствии с пунктом 27 Требований о защите информации. В случае если определенный в установленном порядке уровень защищенности персональных данных выше, чем установленный класс защищенности ГИС, то осуществляется повышение класса защищенности до значения, обеспечивающего выполнение пункта 27 Требований о защите информации.

13. Уровень защищенности персональных данных, обрабатываемых в информационной системе персональных данных Управления, устанавливается комиссией по классификации информационных систем персональных данных Управления в соответствии с Требованиями к защите персональных данных и оформляется актом.

Класс защищенности ГИС Управления, в которой обрабатываются персональные данные, устанавливается комиссией по классификации информационных систем персональных данных Управления в соответствии с пунктом 14.2 Требований о защите информации и оформляется актом классификации.

Комиссия по классификации информационных систем персональных данных Управления создается распоряжением Управления.

14. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Определение типов угроз безопасности персональных данных, актуальных для информационной системы, производится в соответствии с пунктом 7 Требований к защите персональных данных.

Для выбора и реализации в ГИС мер защиты информации в соответствии с пунктом 21 Требований о защите информации применяется методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11.02.2014.

По решению Управления методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11.02.2014, применяется для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, защита которых обеспечивается в соответствии с Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным приказом ФСТЭК России от 18.02.2013 № 21.

Раздел III

Передача служебной информации ограниченного доступа по каналам связи

15. Передача речевой служебной информации ограниченного доступа по открытым проводным каналам связи в Управлении допускается только в пределах контролируемой зоны с использованием внутренней автоматической телефонной станции.

Передача речевой служебной информации ограниченного доступа по радиоканалам, в том числе с использованием мобильных телефонов сотовой связи, и по открытым проводным каналам связи, выходящим за пределы контролируемой зоны, запрещается.

При необходимости такой передачи используются защищенные линии связи, устройства скремблирования или криптографической защиты. Используемые средства защиты информации предварительно должны быть сертифицированы по требованиям безопасности информации.

16. Для передачи служебной информации ограниченного доступа, обрабатываемой в автоматизированных системах, по каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации. Применяемые средства защиты информации должны быть сертифицированы.

17. При передаче персональных данных с использованием автоматизированных систем Управление руководствуется следующими правовыми актами Федеральной службы безопасности Российской Федерации:

приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены руководством 8 Центра Федеральной службы безопасности Российской Федерации 21 февраля 2008 года № 149/54-144);

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены руководством 8 Центра Федеральной службы безопасности Российской Федерации 21.02.2008 № 149/6/6-622).

18. Не допускается подключение информационных систем и информационно-телекоммуникационной сети Управления, применяемых для обработки служебной информации ограниченного доступа, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации

через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети «Интернет».

При необходимости такое подключение производится только с использованием специально предназначенных для этого средств защиты информации. Предварительно данные средства должны пройти обязательную сертификацию в Федеральной службе безопасности Российской Федерации и (или) получить подтверждение соответствия в ФСТЭК России.

Раздел IV Особенности обращения с носителями служебной информации ограниченного доступа

19. В Управлении документы, содержащие служебную информацию ограниченного доступа (далее — документы ограниченного доступа):

1) подготавливаются в автоматизированных системах с соблюдением требований к технической защите служебной информации ограниченного доступа, установленных в разделе II настоящего Положения;

2) передаются по каналам связи с соблюдением требований, установленных пунктами 17 и 18 настоящего Положения;

3) не сканируются и не размещаются в автоматизированной системе «Система электронного документооборота «Дело»;

4) печатаются с указанием на лицевой или оборотной стороне в левом нижнем углу листа (если документ исполнен на одном листе) или в левом углу последнего листа каждого экземпляра документа количества отпечатанных экземпляров, их адреса, учётного номера носителя, с которого произведена печать, фамилии исполнителя, номера его служебного телефона и даты, например:

Отп. 1 экз.
С СМНИ № 1ДСП
Экз. 1 – в адрес.
В.П. Круглов
Тел. (81853) 40000
15.05.2017

или

Отп. 2 экз.
С СМНИ № 1ДСП
Экз. № 1 – в адрес.
Экз. № 2 – в дело.
Владимир Петрович Круглов
Тел. (81853) 40000
15.05.2017;

5) передаются исполнителем после подписания начальником Управления для учета (регистрации) лицу, ответственному за регистрацию данного вида документов ограниченного доступа в Управлении, под личную подпись в учётной форме;

6) учитываются (регистрируются) в учетных формах в соответствии с Инструкцией по делопроизводству в Администрации Ненецкого автономного округа, Аппарате Администрации Ненецкого автономного округа и иных органах исполнительной власти Ненецкого автономного округа, утвержденной постановлением Администрации Ненецкого автономного округа от 27.05.2008 № 80-п;

7) копируются (тиражируются) согласно резолюции начальника Управления или руководителя структурного подразделения, в котором готовился документ. Учет размноженных документов осуществляется поэкземплярно;

8) рассылаются на основании указателя рассылки, подписанного исполнителем документа или руководителем структурного подразделения, ответственного за подготовку документа, в котором поадресно проставляются номера экземпляров отправляемых документов;

9) передаются государственным гражданским служащим Управления (исполнителям) под личную подпись в учетной форме с проставлением на первой странице документа отметки об ознакомлении, в которой указывается фамилия исполнителя и дата ознакомления с документом;

10) пересылаются в органы государственной власти, органы местного самоуправления, организации подразделениями фельдъегерской или специальной связи, заказными или ценными почтовыми отправлениями, а также могут доставляться курьером (нарочным);

11) хранятся в служебных помещениях в надежно запираемых шкафах (ящиках, хранилищах), металлических сейфах. При необходимости шкафы (ящики, хранилища), сейфы и служебные помещения могут опечатываться личными металлическими номерными печатями сотрудников Управления.

20. На документах ограниченного доступа (в необходимых случаях и на их проектах) может ставиться ограничительная пометка «Для служебного пользования» («ДСП»).

Необходимость проставления этой пометки определяется исполнителем и должностным лицом, подписывающим или утверждающим документ.

Пометка «Для служебного пользования» проставляется также на конверте, в котором пересылается документ ограниченного доступа с пометкой «Для служебного пользования».

Регистрационный (учетный) номер документа ограниченного доступа проставляется в позиции, предусмотренной бланком документа, к номеру добавляется пометка «ДСП». Пометка «Для служебного пользования» и номер экземпляра проставляются в правом верхнем углу документа, на обложке и титульном листе документов, а также на первой странице сопроводительного письма к таким документам.

Если конфиденциальный документ не содержит бланка, то его регистрационный (учетный) номер и дата изготовления печатаются в левом верхнем углу документа, а пометка «Для служебного пользования» и номер экземпляра проставляются в правом верхнем углу документа.

21. На съёмных машинных носителях служебной информации ограниченного доступа при необходимости проставляется пометка «Для служебного пользования» («ДСП»).

Учетные реквизиты (учетный номер, дата регистрации, пометка «Для служебного пользования» («ДСП») и так далее) проставляются на съёмных

машинных носителях служебной информации ограниченного доступа любым доступным способом (несмываемый маркер, наклейка и другие) в удобном для просмотра месте, например:

Для служебного пользования
Уч. № 1дсп/МНИ 27.04.2015
Экз. единств.

или

ДСП
Уч. № 1дсп/МНИ 27.04.2015
Экз. единств.

Съемные машинные носители служебной информации ограниченного доступа с пометкой «Для служебного пользования» («ДСП») регистрируются лицом, ответственным за регистрацию данного вида документов ограниченного доступа в Управлении, передаются другим исполнителям под личную подпись в журнале учета машинных носителей информации доступа, уничтожаются по акту.

Рассылка, уничтожение, передача, проверка наличия съемных машинных носителей служебной информации ограниченного доступа в Управлении, проведение расследований по фактам их утраты осуществляется в порядке, установленном для рассылки, уничтожения, передачи, проверки наличия и проведения расследований по фактам утраты документов ограниченного доступа.

22. Исполненные документы ограниченного доступа группируются в дела отдельно или вместе с другими документами по одному и тому же вопросу в соответствии с номенклатурой дел. На обложке дела, в которое помещены документы ограниченного доступа с пометкой «Для служебного пользования», проставляется пометка «Для служебного пользования».

23. Пометка «Для служебного пользования» снимается с документа по окончании срока его хранения согласно утвержденной номенклатуре дел, а с документа длительного или постоянного срока хранения – по истечении 5 лет со дня регистрации. Уничтожение документов, дел и изданий ограниченного доступа, утративших свое практическое значение и не имеющих исторической ценности, производится по акту, который хранится в Управлении. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

24. Проверка наличия документов, дел и изданий ограниченного доступа проводится не реже одного раза в год сотрудником, ответственным за регистрацию данной группы документов ограниченного доступа. При необходимости для проверки может создаваться комиссия, состав которой определяется распоряжением Управления. В состав комиссии включается сотрудник, ответственный за регистрацию данной группы документов ограниченного доступа в Управлении.

25. О фактах утраты документов, дел и изданий ограниченного доступа либо разглашения информации ограниченного доступа сообщается начальнику Управления, который принимает решение о создании комиссии для расследования обстоятельств утраты или разглашения информации ограниченного доступа.

Решение о создании комиссия для расследования обстоятельств утраты или разглашения информации ограниченного доступа оформляется распоряжением Управления.

Результаты расследования представляются начальнику Управления.

26. На утраченные документы, дела и издания ограниченного доступа с пометкой «Для служебного пользования» комиссией, созданной для расследования обстоятельств утраты или разглашения документов, дел и изданий ограниченного доступа составляется акт, на основании которого делаются соответствующие отметки в учетных формах. Акты на утраченные дела постоянного срока хранения после их утверждения передаются в архив.

27. При снятии пометки «Для служебного пользования» на документах, делах и изданиях ограниченного доступа, а также в учетных формах делаются соответствующие отметки и информируются все адресаты, которым эти документы, дела и издания направлялись.

28. Работа с документами ограниченного доступа осуществляется только в служебных помещениях Управления, исключая случайное ознакомление посторонних лиц с документами ограниченного доступа.

29. Допуск к документам ограниченного доступа предоставляется только тем сотрудникам, которым они необходимы для выполнения своих служебных обязанностей.

30. Представители организаций и частные лица могут быть допущены к ознакомлению и работе с документами, делами и изданиями ограниченного доступа по решению начальника Управления, оформленному в письменном виде.

Раздел V

Обязанности и ответственность сотрудников, работающих со служебной информацией ограниченного доступа

31. Сотрудники Управления, работающие со служебной информацией ограниченного доступа, обязаны:

1) знать в части, касающейся исполнения своих должностных обязанностей, перечень служебной информации ограниченного доступа в Управлении, требования настоящего Положения и других правовых актов по защите информации;

2) хранить служебную информацию ограниченного доступа, ставшую им известной по службе (работе), пресекать противоправные действия других сотрудников, которые могут привести к разглашению этой информации, немедленно информировать непосредственного руководителя и ответственного за соблюдение порядка обращения со служебной информацией ограниченного доступа в Управлении о таких фактах, а также о других причинах и условиях возможной утечки служебной информации ограниченного доступа;

3) при увольнении сдать все числящиеся за ним носители служебной информации ограниченного доступа;

4) предъявлять по требованию руководства для проверки все числящиеся и имеющиеся носители служебной информации ограниченного доступа, представлять по требованию руководства устные или письменные объяснения о допущенных нарушениях порядка обращения со служебной информацией

ограниченного доступа, случаях утраты носителей такой информации, а также о случаях утраты ключей, печатей от помещений, в которых проводится работа со служебной информацией ограниченного доступа, в том числе автоматизированная обработка, и совещания с ее обсуждением;

5) вести переговоры, связанные с обсуждением служебной информации ограниченного доступа, только по защищенным линиям связи;

6) сообщать служебную информацию ограниченного доступа при обращении по личным вопросам, с жалобами, просьбами и предложениями в государственные органы и органы местного самоуправления, общественные объединения (в случае возникновения необходимости изложить указанную информацию необходимо руководствоваться требованиями настоящего Положения);

7) при убытии в отпуск или командировку обеспечить доступ к документам ограниченного доступа, находящимся в работе, своему непосредственному руководителю или сотруднику, замещающему лицо, работающее с документами ограниченного доступа.

32. Сотрудники Управления несут дисциплинарную или иную предусмотренную законодательством Российской Федерации ответственность за несоблюдение требований настоящего Положения.

Приложение 2
к приказу Управления по
государственному регулированию цен
(тарифов) Ненецкого автономного
округа от 26.06.2017 № 11
«О порядке обращения со служебной
информацией ограниченного доступа
в Управлении по государственному
регулированию цен (тарифов)
Ненецкого автономного округа»

Инструкция
по обработке информации ограниченного доступа
с использованием средств вычислительной техники
в Управлении по государственному регулированию
цен (тарифов) Ненецкого автономного округа

1. Настоящая инструкция, разработанная в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Положением о порядке обращения со служебной информацией ограниченного доступа в Управлении по государственному регулированию цен (тарифов) Ненецкого автономного округа (далее – Управление), определяет порядок обработки информации ограниченного доступа, не отнесенной к сведениям, составляющим государственную тайну (далее – служебная информация ограниченного доступа), с использованием средств вычислительной техники (далее – СВТ) в Управлении.

2. Обработка служебной информации ограниченного доступа должна производиться на СВТ, оснащенных системой защиты информации, в составе которой присутствуют система защиты информации от несанкционированного доступа и сертифицированное антивирусное программное обеспечение. В СВТ должны отсутствовать любые радиоинтерфейсы (беспроводные сетевые адаптеры, Bluetooth-адаптеры, GSM/GPRS/UMTS/LTE-модемы и т.п.)

3. СВТ, на котором производится обработка служебной информации ограниченного доступа, должно быть установлено таким образом, чтобы исключить несанкционированный просмотр выводимой на нем информации. В момент обработки служебной информации ограниченного доступа в помещении не должно находиться посторонних лиц, не допущенных к данной информации.

4. Не допускается обработка служебной информации ограниченного доступа на СВТ, подключенных (или имеющих возможность подключения) к информационно-телекоммуникационной сети Управления и к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети «Интернет».

5. В случае если рабочее место не позволяет организовать выделенное СВТ для обработки служебной информации ограниченного доступа, перед началом

обработки служебной информации ограниченного доступа на своём рабочем месте необходимо произвести следующие действия:

1) отключить используемое СВТ от информационно-телекоммуникационной сети Управления путем физического извлечения Ethernet-кабеля из разъема СВТ;

2) извлечь из СВТ все съемные машинные носители информации (CD/DVD диски, Flash-накопители, внешние жесткие диски и т.п.), не требуемые для обработки служебной информации ограниченного доступа;

3) извлечь из разъемов СВТ любые USB-устройства, использующие радиointерфейсы (мобильные телефоны, USB-модемы, Bluetooth-адаптеры и т.п.);

4) убедиться, что антивирусное программное обеспечение включено (резидентный модуль «Монитор») и имеет актуальную базу данных угроз;

5) при планируемом выводе на печать документов, содержащих служебную информацию ограниченного доступа, убедиться, что используемый принтер имеет прямое проводное подключение к СВТ и не является сетевым;

6) убедиться, что в оперативной памяти СВТ не загружены прикладные программные средства, не участвующие в обработке служебной информации ограниченного доступа (путем просмотра «Диспетчера задач»).

6. Создание, редактирование, хранение электронных версий документов (черновиков), содержащих служебную информацию ограниченного доступа допускается только на съемных машинных носителях служебной информации, учтенных в соответствии с Приложением 1 к настоящему приказу.

7. Для передачи служебной информации ограниченного доступа, обрабатываемой в автоматизированных системах, по каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации. Применяемые средства защиты информации должны быть сертифицированы.

8. По окончании обработки служебной информации ограниченного доступа необходимо произвести стирание остаточной информации на несъемных носителях (жестких дисках) и в оперативной памяти. Стирание остаточной информации в оперативной памяти производится путем перезагрузки ПЭВМ.

9. Отпечатанные на бумажных носителях документы, содержащие служебную информацию ограниченного доступа, регистрируются и учитываются в соответствии с Приложением 1 к настоящему приказу.

10. Хранение учтенных съемных машинных носителей служебной информации производится в служебных помещениях в надежно запираемых шкафах (ящиках, хранилищах), металлических сейфах. При необходимости шкафы (ящики, хранилища), сейфы и служебные помещения могут опечатываться личными металлическими номерными печатями сотрудников Управления.

11. Контроль за исполнением настоящей инструкции осуществляет начальник Управления.

Приложение 3
к приказу Управления по
государственному регулированию цен
(тарифов) Ненецкого автономного
округа от 26.06.2017 № 11
«О порядке обращения со служебной
информацией ограниченного доступа
в Управлении по государственному
регулированию цен (тарифов)
Ненецкого автономного округа»

**Примерный перечень
служебной информации ограниченного доступа
в Управлении по государственному
регулированию цен (тарифов)
Ненецкого автономного округа**

I. Вопросы мобилизационной подготовки, мобилизации

1. Обобщенные сведения по вопросам мобилизационной подготовки и мобилизации в Управлении по государственному регулированию цен (тарифов) Ненецкого автономного округа (далее – Управление), не содержащие сведений, отнесенных к государственной тайне.

2. Переписка, планирование и отчетность, не содержащая сведений, отнесенных к государственной тайне, по вопросам мобилизационной подготовки и мобилизации в Управлении.

II. Вопросы информатизации и защиты информации

3. Сведения, раскрывающие в Управлении систему и средства защиты информации в автоматизированных системах.

4. Сведения об организации системы разграничения доступа к защищаемым информационным ресурсам, о действующих паролях, закрытых ключах электронно-цифровой подписи, ключах шифрования информации, если они не относятся к сведениям, составляющим государственную тайну.

5. Сведения об объектах информатизации Управления, в которых обрабатывается информация с ограниченным доступом.

6. Сведения об организации защиты информации на объектах информатизации Управления, в которых обрабатывается информация с ограниченным доступом.

7. Сведения о результатах контроля состояния защиты информации в Управлении, эффективности применяемых мер и средств защиты информации на объектах информатизации Управления, в которых обрабатывается информация с ограниченным доступом.

III. Персональные данные

8. Персональные данные лиц, замещающих в Управлении должности государственной гражданской службы Ненецкого автономного округа.

9. Персональные данные членов семей лиц, замещающих в Управлении должности государственной гражданской службы Ненецкого автономного округа.

10. Персональные данные граждан, обратившихся в Управление в соответствии с Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

11. Сведения о государственных гражданских служащих, содержащиеся в автоматизированной системе «1С: Предприятие 8.3».

12. Сведения, содержащие по совокупности штатное расписание, списки телефонов, с указанием домашних телефонов и занимаемых должностей государственных гражданских служащих Управления.

IV. Прочие сведения

13. Переписка, планирование и отчетность, не содержащая сведений, отнесенных к государственной тайне, по вопросам противодействия экстремизму и терроризму, коррупции.

14. Сведения, содержащиеся в регистрах бухгалтерского учета, внутренней бухгалтерской отчетности Управления (коммерческая тайна).

15. Сведения, составляющие служебную тайну органов государственной власти, органов местного самоуправления, организаций, переданные в исполнительные органы.

16. Сведения, связанные с профессиональной деятельностью (тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений).

17. Сведения о прогнозах и результатах финансово-хозяйственной деятельности организаций, за исключением сведений, которые не могут составлять коммерческую тайну.

18. Сведения о целях, рассматриваемых вопросах, результатах, фактах проведения совещаний, заседаний и переговоров по конфиденциальным вопросам.

19. Другие служебные сведения, доступ к которым ограничен в соответствии с федеральным законом.
