Департамент цифрового развития, связи и массовых коммуникаций Ненецкого автономного округа

ПРИКАЗ

от 19 июня 2019 г. № 37
г. Нарьян-Мар

О порядке обращения со служебной информацией ограниченного доступа в Департаменте цифрового развития, связи и массовых коммуникаций Ненецкого автономного округа

В соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», ПРИКАЗЫВАЮ:

1. Утвердить:

1) Положение о порядке обращения со служебной информацией ограниченного доступа в Департаменте цифрового развития, связи и массовых коммуникаций Ненецкого автономного округа согласно Приложению 1;

2) Инструкцию по обработке информации ограниченного доступа с использованием средств вычислительной техники в Департаменте цифрового развития, связи и массовых коммуникаций Ненецкого автономного округа согласно Приложению 2.

3) Примерный перечень служебной информации ограниченного доступа в Департаменте цифрового развития, связи и массовых коммуникаций Ненецкого автономного округа согласно Приложению 3.

4) Журнал регистрации документов для служебного пользования согласно Приложению 4.

5) Журнал учёта съёмных магнитных носителей информации согласно Приложению 5.

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

Исполняющий обязанности
руководителя Департамента
цифрового развития, связи
и массовых коммуникаций
Ненецкого автономного округа М.А. Марков

Приложение 1
к приказу Департамента
цифрового развития, связи
и массовых коммуникаций
Ненецкого автономного округа
от 19.06.2019 № 37
«О порядке обращения
со служебной информацией
ограниченного доступа
в Департаменте цифрового
развития, связи и массовых
коммуникаций Ненецкого
автономного округа»

Положение о порядке обращения со служебной информацией ограниченного доступа в Департаменте цифрового развития, связи и массовых коммуникаций Ненецкого автономного округа

Раздел I
Общие положения

1. Настоящее Положение, разработанное в соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», определяет общий порядок обращения с документами на различных носителях информации, 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 Департаменте цифрового развития, связи и массовых коммуникаций Ненецкого автономного округа (далее – Департамент).

2. К служебной информации ограниченного доступа в Департаменте относится служебная информация, не отнесенная к сведениям, составляющим государственную тайну, используемая в деятельности Департамента, 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 Департаменте принимаются правовые, организационные, технические и иные меры защиты информации.

3. Содержание сведений, которые относятся к служебной информации ограниченного доступа в соответствии с федеральными законами, устанавливающими условия отнесения информации к сведениям, составляющим служебную тайну, определяется Примерным перечнем служебной информации ограниченного доступа в Департаменте, утверждаемым правовым актом Департамента.

Перечень не ограничивает право отнесения не вошедших в него сведений к служебной информации ограниченного доступа, если это не противоречит

федеральным законам.

4. Не может быть ограничен доступ к:

нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

информации о состоянии окружающей среды;

информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

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;

съемный 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;

защищаемые помещения (далее - ЗП) - кабинеты, предназначенные для проведения совещаний, связанных с обсуждением служебной информации ограниченного доступа;

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 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».

6. Ответственность за организацию порядка обращения со служебной информацией ограниченного доступа в Департаменте возлагается на организационно-правовой сектор комитета финансового и правового обеспечения Департамента.

7. В Департаменте назначаются государственные гражданские служащие, ответственные за соблюдение порядка обращения со служебной информацией ограниченного доступа. Все входящие и исходящие документы, содержащие служебную информацию ограниченного доступа, ответственными лицами регистрируются в журнале согласно Приложению 4.

8. Методическую помощь по решению вопросов технической защиты служебной информации ограниченного доступа в Департаменте оказывает сектор защиты информации Аппарата Администрации Ненецкого автономного округа.

9. Для оказания услуг в области защиты служебной информации ограниченного доступа Департаментом 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 Департамента решение о дальнейшем использовании носителей служебной информации ограниченного доступа, имеющихся в структурных подразделениях Департамента, принимает комиссия, создаваемая распоряжением Департамента.

Раздел II
Техническая защита служебной информации ограниченного доступа

11. Техническая защита служебной информации ограниченного доступа в Департаменте осуществляется во взаимодействии с казенным учреждением Ненецкого автономного округа «Ненецкий информационно-аналитический центр» в соответствии с законодательством Российской Федерации, стандартами и иными правовыми актами Федеральной службы по техническому и экспортному контролю России (далее - ФСТЭК России) в области защиты информации, а также настоящим Положением.

12. В целях подтверждения эффективности системы защиты информации в Департаменте может проводиться аттестация ЗП на соответствие требованиям безопасности информации.

Аттестация ЗП проводится в соответствии со Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2002 № 282, национальными стандартами ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения» и ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».

13. Программа аттестационных испытаний ЗП согласовывается с сектором защиты информации Аппарата Администрации Ненецкого автономного округа.

14. Ввод в действие ЗП осуществляется после его аттестации по требованиям

безопасности информации на основании выданного аттестата соответствия.

Разрешение о вводе в действие ЗП принимается и документально оформляется распоряжением Департамента.

15. Создание систем защиты персональных данных, обрабатываемых в информационных системах персональных данных Департамента, 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 Департамента (далее - ГИС) осуществляется в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, 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.

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

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

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

17. 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 от 27.07.2006 № 152-ФЗ «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 Департамента 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, утвержденными приказом ФСТЭК России от 18.02.2013 № 21.

18. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных проводится до ввода в эксплуатацию информационной системы персональных данных Департаментом самостоятельно или с привлечением юридических лиц, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

Решение по форме оценки эффективности и документов, разрабатываемых по результатам (в процессе) оценки эффективности, принимается Департаментом самостоятельно и (или) по соглашению с лицом, привлекаемым для проведения оценки эффективности реализованных мер по обеспечению безопасности персональных данных.

Оценка эффективности реализованных мер может быть проведена в рамках работ по аттестации информационной системы персональных данных в соответствии с национальным стандартом ГОСТ РО 0043-003-2012.

В части ГИС, в которых обрабатываются персональные данные, оценка эффективности принимаемых мер по обеспечению безопасности персональных данных проводится в рамках обязательной аттестации ГИС по требованиям защиты информации в соответствии с Требованиями о защите информации, национальными стандартами ГОСТ РО 0043-003-2012 и ГОСТ РО 0043-004-2013. Указанная аттестация проводится не реже одного раза в 3 года.

Раздел III
Передача служебной информации ограниченного доступа по каналам связи

19. Передача речевой служебной информации ограниченного доступа по открытым проводным каналам связи в Департаменте 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 должны быть сертифицированы по требованиям безопасности информации.

20. 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.

При передаче персональных данных с использованием автоматизированных систем необходимо руководствоваться следующими актами Федеральной службы безопасности Российской Федерации:

приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава 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 21.02.2008 № 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).

21. Не допускается подключение информационных систем и информационно-телекоммуникационной сети Департамента, 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

22. В Департаменте 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 20 и 21 настоящего Положения;

3) не должны сканироваться и размещаться 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, учетного номера носителя, с которого произведена печать, фамилии исполнителя, номера его служебного телефона и даты, например:

Отп. 1 экз.
С СМНИ № 2ДСП
Экз. № 1 - в адрес.
В.П. Круглов
Тел. (81853) 40000
15.11.2017

или

Отп. 2 экз.
С СМНИ № 5ДСП
Экз. № 1 - в адрес.
Экз. № 2 - в дело.
Владимир Петрович Круглов
Тел. (81853) 40000
15.11.2017;

5) передаются после подписания руководителем для учета (регистрации) лицу, ответственному за регистрацию данного вида документов ограниченного доступа в Департаменте, под личную подпись в учетной форме;

6) учитываются (регистрируются) в учетных формах в соответствии с Инструкцией по делопроизводству в Администрации Ненецкого автономного округа и иных исполнительных органах государственной власти Ненецкого автономного округа, утвержденной постановлением Администрации Ненецкого автономного округа от 15.05.2018 № 110-п;

7) копируются (тиражируются) согласно резолюции соответствующего руководителя или руководителя структурного подразделения, в котором готовился документ, с осуществлением поэкземплярного учета размноженных документов;

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 Департамента (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, которые при необходимости могут опечатываться личными металлическими номерными печатями сотрудников Департамента.

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

Необходимость проставления пометки «Для служебного пользования» определяется лицом, подготовившим документ, 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.

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

Для служебного пользования
Уч. № 13дсп/МНИ 27.04.2011
Экз. единств.

или

ДСП
Уч. № 13дсп/МНИ 27.04.2011
Экз. единств.

25. Съемные машинные носители служебной информации ограниченного доступа с пометкой «Для служебного пользования» («ДСП») регистрируются лицом, ответственным за регистрацию данного вида документов ограниченного доступа в Департаменте, передаются исполнителям под личную подпись в журнале учета машинных носителей информации доступа, согласно Приложению 5, уничтожаются по акту.

Рассылка, уничтожение, передача, проверка наличия съемных машинных носителей служебной информации ограниченного доступа в Департаменте,

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.

26. 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».

27. 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 Департаменте. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

28. 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 Департамента. В состав комиссии включается сотрудник, ответственный за регистрацию данной группы документов ограниченного доступа в Департаменте.

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

Решение о создании комиссии для расследования обстоятельств утраты или разглашения информации ограниченного доступа оформляется распоряжением Департамента.

Результаты расследования представляются руководителю Департамента.

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

31. 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.

32. Работа с документами ограниченного доступа осуществляется только в служебных помещениях Департамента в условиях, исключающих случайное ознакомление посторонних лиц с документами ограниченного доступа.

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

34. Представители организаций и частные лица могут быть допущены

к ознакомлению и работе с документами, делами и изданиями ограниченного доступа по решению руководителя Департамента, оформленному в письменной форме.

Раздел V
Обязанности и ответственность сотрудников, работающих со служебной информацией ограниченного доступа

35. Сотрудники Департамента, работающие со служебной информацией ограниченного доступа, обязаны:

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

2) хранить в соответствии с установленными требованиями 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 Департаменте 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 непосредственного или вышестоящего руководителя для проверки все числящиеся и имеющиеся носители служебной информации ограниченного доступа, а также 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 передачей служебной информации ограниченного доступа, только по защищенным линиям связи;

6) при убытии в отпуск или командировку обеспечить доступ к документам ограниченного доступа, находящимся в работе, своему непосредственному руководителю или сотруднику, на которого возложено исполнение обязанностей временно отсутствующего работника, осуществляющего работу с документами ограниченного доступа.

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

Приложение 2
к приказу Департамента
цифрового развития, связи
и массовых коммуникаций
Ненецкого автономного округа
от 19.06.2019 № 37
«О порядке обращения
со служебной информацией
ограниченного доступа
в Департаменте цифрового
развития, связи и массовых
коммуникаций Ненецкого
автономного округа»

Инструкция по обработке информации ограниченного доступа с использованием средств вычислительной техники в Департаменте цифрового развития, связи и массовых коммуникаций Ненецкого автономного округа согласно

1. Настоящая Инструкция, разработанная в соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», 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 Департаменте.

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 должны находиться посторонние лица, не имеющие допуска к данной информации.

4. Не допускается обработка служебной информации ограниченного доступа на СВТ, подключенных (или имеющих возможность подключения) к информационно-телекоммуникационной сети Департамента 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 своем рабочем месте

необходимо произвести следующие действия:

1) отключить используемое СВТ от информационно-телекоммуникационной сети Департамента 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 используемые для обработки служебной информации ограниченного доступа;

3) извлечь из разъемов СВТ любые USB-устройства, использующие радиоинтерфейсы (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 персональной электронно-вычислительной машины.

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 Департамента.

11. Контроль за соблюдением требований настоящей инструкции осуществляют сотрудники организационно-правового сектора комитета финансового и правового обеспечения Департамента.

Приложение 3
к приказу Департамента
цифрового развития, связи
и массовых коммуникаций
Ненецкого автономного округа
от 19.06.2019 № 37
«О порядке обращения
со служебной информацией
ограниченного доступа
в Департаменте цифрового
развития, связи и массовых
коммуникаций Ненецкого
автономного округа»

Примерный перечень служебной информации ограниченного доступа в Департаменте цифрового развития, связи и массовых коммуникаций Ненецкого автономного округа

1. К служебной информации ограниченного доступа по вопросам мобилизационной подготовки относится следующая информация:

1) обобщенные сведения о наличии, качественном состоянии защитных сооружений и других объектов гражданской обороны на территории Ненецкого автономного округа, не содержащие сведений, отнесенных к государственной тайне;

2) обобщенные сведения о транспортных средствах в Ненецком автономном округе, используемых в интересах проведения мероприятий гражданской обороны, не содержащие сведений, отнесенных к государственной тайне;

3) обобщенные сведения по Ненецкому автономному округу по вопросам организации и проведения эвакуационных мероприятий в военное время, не содержащие сведений, отнесенных к государственной тайне;

4) переписка, планирование и отчетность, не содержащая сведений, отнесенных к государственной тайне, по вопросам:

мобилизационной подготовки и мобилизации экономики Ненецкого автономного округа;

воинского учета и бронирования граждан, пребывающих в запасе;

5) сведения об организациях, ведущих бронирование граждан, пребывающих в запасе Вооруженных Сил Российской Федерации, на период мобилизации и на военное время пребывающих в запасе.

2. К служебной информации ограниченного доступа по вопросам информатизации и защиты информации относится следующая информация:

1) сведения, раскрывающие систему и средства защиты информации в автоматизированных системах Департамента;

2) 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;

3) сведения об объектах информатизации Департамента, в которых обрабатывается информация с ограниченным доступом;

4) сведения об организации защиты информации на объектах информатизации Департамента, в которых обрабатывается (обсуждается) информация с ограниченным доступом;

5) сведения о результатах контроля состояния защиты информации в Департаменте, эффективности применяемых мер и средств защиты информации на объектах информатизации, в которых обрабатывается информация с ограниченным доступом.

3. К служебной информации ограниченного доступа относятся следующие персональные данные, обрабатываемые в Департаменте:

1) персональные данные на лиц, замещающих должности государственной гражданской службы в Департаменте, и лиц, замещающих должности в Департаменте, не являющиеся должностями государственной гражданской службы, а также руководителей подведомственных Департаменту организаций (включая сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, в том числе документы, содержащие сведения, отнесенные к банковской и коммерческой тайне);

2) персональные данные членов семей лиц, замещающих должности государственной гражданской службы в Департаменте, и лиц, замещающих должности в Департаменте, не являющиеся должностями государственной гражданской службы, а также руководителей подведомственных Департаменту организаций (включая сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, в том числе документы, содержащие сведения, отнесенные к банковской и коммерческой тайне);

3) персональные данные, внесенные в документы учета лиц, замещающих должности государственной гражданской службы в Департаменте, и лиц, замещающих должности в Департаменте, не являющиеся должностями государственной гражданской службы, а также руководителей подведомственных Департаменту организаций;

4) персональные данные граждан, обратившихся в Департамент в соответствии с федеральным законом;

5) сведения о лицах, содержащиеся в автоматизированных бухгалтерских и иных системах Департамента;

6) сведения, содержащие по совокупности штатное расписание, списки телефонов, с указанием домашних телефонов и занимаемых должностей лиц, замещающих должности государственной гражданской службы в Департаменте, и лиц, замещающих должности в Департаменте, не являющиеся должностями государственной гражданской службы, а также руководителей подведомственных Департаменту организаций;

7) иные сведения о персональных данных лиц, обрабатываемых в Департаменте в рамках действующих полномочий.

4. Помимо информации, указанной в пунктах 1 - 3 настоящего Примерного перечня, к служебной информации ограниченного доступа в Департаменте относятся:

1) переписка, планирование и отчетность, не содержащая сведений, отнесенных к государственной тайне, по вопросам:

противодействия экстремизму и терроризму, незаконному обороту наркотических средств и психотропных веществ;

обеспечения общественного порядка;

допризывной подготовки и призыва граждан на военную службу;

противодействия коррупции (включая документы по вопросам взаимодействия с правоохранительными и контрольно-надзорными органами Ненецкого автономного округа);

2) информация о новых решениях и технических знаниях, полученных благодаря исполнению обязательств по договору, в том числе не защищаемых законом, а также сведения, которые могут рассматриваться как коммерческая тайна;

3) сведения, содержащиеся в регистрах бухгалтерского учета, внутренней бухгалтерской отчетности Департамента;

4) сведения о порядке и состоянии организации охраны, пропускном режиме, применяемых системах и средствах охранной, тревожной, пожарной сигнализации и видеонаблюдения служебных помещений, в которых размещается Департамент, планах их усовершенствования;

5) сведения, составляющие служебную тайну органов государственной власти, органов местного самоуправления, организаций, переданные в Департамент;

6) сведения, связанные с профессиональной деятельностью (тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений);

7) сведения о целях, рассматриваемых вопросах, результатах, фактах проведения совещаний, заседаний и переговоров по конфиденциальным вопросам;

8) другие служебные сведения, доступ к которым ограничен в соответствии с федеральным законом.

Приложение 4
к приказу Департамента
цифрового развития, связи
и массовых коммуникаций
Ненецкого автономного округа
от 19.06.2019 № 37
«О порядке обращения
со служебной информацией
ограниченного доступа
в Департаменте цифрового
развития, связи и массовых
коммуникаций Ненецкого
автономного округа»

Журнал регистрации документов для служебного пользования

Дата уч. №	Корреспондент (исполнитель)	Наименование (содержание) документа	Адресат
1	2	3	4

Приложение 5
к приказу Департамента
цифрового развития, связи
и массовых коммуникаций
Ненецкого автономного округа
от 19.06.2019 № 37
«О порядке обращения
со служебной информацией
ограниченного доступа
в Департаменте цифрового
развития, связи и массовых
коммуникаций Ненецкого
автономного округа»

Журнал учёта съёмных магнитных носителей информации

Рег. номер, отр. отметка	Дата постановки на учёт	Откуда поступил	Тип машинного носителя	Ответственный за хранение (место хранения), адрес отсылки	Категория информации на носителе	Отметка о получении носителя		Отметка об обратном приеме носителя	Отметка об уничтожении носителя
						дата	Фамилия, подпись		
1	2	3	4	5	6	7	8	9	10