

Муниципальное бюджетное дошкольное образовательное учреждение
детский сад № 27 села Молдаванского муниципального образования
Крымский район

ПРИКАЗ

От 09.01.2020 г.

№ 42/1-од

с. Молдаванское

**«Об утверждении документов, направленных на обеспечение
выполнения обязанностей, предусмотренных Федеральным законом «О
персональных данных» и принятыми в соответствии с ним
нормативными актами»**

В целях обеспечения выполнения обязанностей, предусмотренных Федеральным Законом Российской Федерации от 27 июля 2006г. №152-ФЗ «О персональных данных» и Постановлением Правительства Российской Федерации от 21.03.2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» в МБДОУ детском саду №27, приказываю:

1. Утвердить и ввести в действие с 09.01.2020 года следующие документы, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» от 27.06.2006г. №152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, в МБДОУ детском саду № 27:

- Регламент использования электронной почты в МБДОУ детском саду №27;
- Приложение №1: памятка по работе с корпоративной электронной почтой.
- Регламент использования сотрудниками ресурсов сети Интернет.
- Порядок уничтожения, блокирования персональных данных.
- Требования к оборудованию помещений и размещению технических средств, используемых для обработки персональных данных.

2. Приказ вступает в силу со дня его подписания.

3. Контроль за исполнением приказа оставляю за собой.

Заведующий МБДОУ детский сад № 27



Н.И.Кайшева

УТВЕРЖДАЮ
Заведующий МБДОУ
детского сада № 27

2020 г.

Н.И. Кайшева



ПОРЯДОК

Уничтожения, блокирования персональных данных

1. Общие положения

Настоящий Порядок определяет условия и способы:

- уничтожения бумажных носителей, документов, содержащих персональные данные по достижению цели обработки этих персональных данных;

- персональных данных в машинных носителях информации, в том числе персональных данных, и при необходимости самих машинных носителей информации.

2. Блокирование и уничтожение персональных данных, содержащихся в машинных носителях информации

2.1. блокирование информации, содержащей персональные данные субъекта персональных данных, производится в случаях:

- если перс. данные являются не полными, устаревшими, не достоверными;
- если сведения являются не законно полученными или не являются не обходимыми для заявленной оператором персональных данных цели обработки.

2.2. в случае подтверждения факта недостоверности персональных данных уполномоченное лицо на основании документов, представленных субъектом персональных данных, уполномоченным органом по защите прав субъектов персональных данных или полученных в ходе самостоятельной проверки, обязано уточнить персональные данные и снять их блокирование.

2.3. в случае выявления неправомерных действий с персональными данными уполномоченное лицо обязано устранить (организовать устранения) допущенные нарушения. В случае невозможности устранения допущенных нарушений необходимо в срок, не превышающий 3 рабочих дней с датой выявления неправомерности действий с персональными данными уничтожить персональные данные.

2.4. об устранении допущенных нарушений или об уничтожении персональных данных уполномоченное лицо обязано уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, так же указанный орган.

2.5. уполномоченное лицо обязано уничтожить персональные данные субъекта персональных данных в случаях:

- достижения цели обработки персональных данных оператор;
- отзыва субъектом согласия на обработку своих персональных данных.

2.6. уничтожение персональных данных должно быть осуществлено в течение 3-х дней с указанных моментов. В согласии субъекта персональных данных на обработку его персональных данных могут быть установлены иные сроки уничтожения персональных данных при достижении цели обработки персональных данных.

3. Работа с бумажными носителями (документами)

3.1. виды и периоды уничтожения бумажных носителей, содержащих персональные данные, представлены в таблице 1:

Таблица 1. Виды и периоды уничтожения бумажных носителей, содержащих персональные данные

№ п/п	Документ	Срок хранения	Действия по окончании срока хранения
1.	Документы (сведения, содержащие персональные данные о работниках), переданные и сформированные при трудоустройстве работника.	75 лет	Уничтожение
2.	Документы о воспитанниках (сведения, содержащие персональные данные обучающихся).	установленные для данных документов сроки хранения	Уничтожение
3.	Другие документы с грифом «Конфиденциально» и «Для служебного пользования» (Журналы учёта, списки доступа, эксплуатационная документация и т.п.)	хранятся до замены на новые, если не указан конкретный срок	Уничтожение

3.2 Документы, указанные в п. 3.1., должны находиться в сейфах, или в закрывающихся металлических шкафах. Исключение составляют документы, обрабатываемые в настоящий момент на рабочем месте.

3.3. По окончании срока хранения документы, указанные в п. 3.1., уничтожаются путём измельчения на мелкие части (или иным способом), исключающие возможность последующего восстановления информации или сжигаются.

4. Работа с машинными носителями информации

4.1. Виды и периоды уничтожения персональных данных, хранимых в электронном виде («файлах») на жестком диске компьютера (далее – НЖМД) и машинных носителях: компакт дисках (далее – CD-R/RW, DVD-R/RW в

зависимости от формата), FLASH-накопителях. Пример видов и периодов уничтожения персональных данных, хранимых в электронном виде на НЖМД, представлен в таблице 2.

Таблица 2

Виды и периоды уничтожения персональных данных, хранимых в электронном виде на жестком диске компьютера

№ п/п	Информация, вид носителя	Срок хранения	Действия по окончании срока хранения
1.	База данных автоматизированной информационной системы Оператора. Носитель: файлы на НЖМД сервера	До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности – уничтожение носителя; удаление архивных файлов с НЖМД

4.2. Машинные носители информации (за исключением НЖМД), перечисленные в п.п. 3.1. должны находиться в сейфе или в закрывающемся металлическом шкафу (кроме формируемых или обрабатываемых в данный момент на рабочем месте).

4.3. По окончании указанных сроков хранения, машинные носители информации, подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления и дальнейшего использования. Это достигается путём деформирования, нарушения единой целостности носителя или его сжигания.

4.4. Подлежащие уничтожению файлы, расположенные на жестком диске ПЭВМ, удаляются средствами операционной системы с последующим «очищением корзины».

4.4. В случае допустимости повторного использования носителя формата FDD, CD-RW, DVD-RW, FLASH применяется программное удаление

(«затирание») содержимого диска путём его форматирования с последующей записью новой информации на данный носитель.

5. Порядок оформления документов об уничтожении носителей

5.1. Уничтожение носителей, содержащих персональные данные, осуществляет специальная Комиссия, создаваемая приказом руководителя.

5.2. В ходе процедуры уничтожения персональных данных носителей необходимо присутствие членов Комиссии, осуществляющей уничтожение персональных данных и иной конфиденциальной информации, находящейся на технических средствах.

5.3. Комиссия составляет и подписывает Акт (2экземпляра) об уничтожении носителей. В течение трёх дней после составления акты об уничтожении направляются на утверждение руководителю. После утверждения один экземпляр Акта хранится у руководителя соответствующего подразделения, второй экземпляр Акта хранится у заведующего.

**Муниципальное бюджетное дошкольное образовательное
учреждение детский сад № 27 села Молдаванского
муниципального образования Крымский район
(МБДОУ детский сад № 27)**

Утверждаю

Заведующий

МБДОУ детского сада № 27

Н.И.Кайшева

Приказ № *477* от *29.08.2018*



Регламент использования сотрудниками ресурсов сети Интернет

1. Общие положения

1.1. Настоящий Регламент разработан для повышения эффективности работы сотрудников МБДОУ детского сада №27 (далее-ДОО),

Использующих электронные информационные ресурсы глобальной сети Интернет, и повышения уровня информационной безопасности локальной информационно-вычислительной сети ДОО.

1.2. Заведующий ДОО устанавливает постоянный контроль за доступом работников к сети Интернет. В случае нарушения сотрудником ДОО данного Регламента работник будет отстранен от использования ресурсов сети Интернет.

2. Назначение доступа к ресурсам сети Интернет

2.1. Доступ к ресурсам сети Интернет предоставляется сотрудникам ДОО для выполнения ими прямых должностных обязанностей. Глобальная информационная сеть Интернет используется для:

- доступа к мировой системе гипертекстовых страниц (www);-доступа к файловым ресурсам Интернета (FTP)
- доступа к специализированным (правовым и др.) базам данных;

- контактов с официальными лицами правительственных структур, с подрядчиками и обслуживающими организациями;
- обмена электронной почтой с официальными лицами по неконфиденциальным вопросам производственного характера;
- повышения квалификации работников, необходимой для выполнения работником своих должностных обязанностей;
- поиска и сбора информации по управленческим, производственным, финансовым, юридическим вопросам, если эти вопросы напрямую связаны с выполнением работником его должностных обязанностей;
- другие цели.

3. Доступ к интернет-ресурсам

3.1. ДОО обеспечивает доступ пользователей локальной сети к ресурсам сети Интернет по специальным каналам связи в соответствии с настоящим Регламентом.

4. Ограничения при работе в сети Интернет

4.1. Пользователям корпоративной линии подключения ДОО к ресурсам глобальной сети Интернет не рекомендуется:

посещение и использование игровых, развлекательных и прочих сайтов, не имеющих отношения к деятельности ДОО и деятельности пользователя;

использование электронной почты, досок объявлений, конференций на компьютерах ДОО в личных целях в любое время;

публикация корпоративного электронного адреса на досках объявлений, в конференциях и гостевых книгах;

использование некорпоративных e-mail адресов для рассылки служебной информации;

передача учетных данных пользователя;

применение имен пользователей и паролей компьютеров ДОО на иных (сторонних) компьютерах;

играть в рабочее время в компьютерные игры автономно или в сети; единовременное скачивание больших объемов информации (файлы в объемах, превышающих указанные в приложении к настоящему Регламенту);

посещение ресурсов трансляции потокового видео и аудио (веб-камеры, трансляция ТВ - и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;

подключение к электронной сети под другим паролем;

создание личных веб-страниц и хостинг (размещение web- или ftp-сервера) на компьютере пользователя.

4.2. Пользователям корпоративной линии подключения ДОО к ресурсам глобальной сети Интернет запрещается:

посещение и использование эротико-порнографических ресурсов сети Интернет, ресурсов националистических организаций, ресурсов, пропагандирующих насилие и терроризм;

нарушение закона об авторском праве посредством копирования и использования в служебных или личных целях материалов, защищенных законом об авторском праве;

осуществление деструктивных действий по отношению к нормальной работе электронной системы Предприятия и сети Интернет (рассылка вирусов, ip-атаки и т.п.);

загрузка материалов порнографического содержания, компьютерных игр, анекдотов, других развлекательных материалов;

передача персональных данных, конфиденциальной информации, сведений, составляющих служебную и коммерческую тайну, третьей стороне;

нанесение вреда электронной системе МПР России; проведение незаконных операций в глобальной сети Интернет; совершение иных действий, противоречащих законодательству, а также настоящему Регламенту.

5. Обращение в другие организации от имени ДОО

5.1. Работа в сети Интернет, общение с другими организациями могут быть связаны с необходимостью изложения своих взглядов по отдельным

вопросам. Если сотрудник ДОО высказывает в сообщении собственное мнение, то указанный сотрудник обязан предупредить об этом в конце сообщения фразой: «Прошу считать, что в сообщении указано мое личное мнение, которое необязательно отражает взгляды и политику ДОО» – по предварительному согласованию с заведующим.

5.2. Официальные обращения по электронной почте к должностным лицам организаций-партнеров и организаций-заказчиков продукции и услуг ДОО осуществляются по указанию заведующего, заместителя заведующего по АХР, старшего воспитателя.

6. Время работы пользователей в сети Интернет

6.1. Время работы пользователей в сети Интернет регламентировано следующим образом: с понедельника по пятницу, с 08.00 до 17.00; при необходимости работы с ресурсами сети Интернет в выходные дни или в вечернее время пользователь обязан получить разрешение у заведующего.

7. Контроль использования ресурсов сети Интернет

7.1. Администрация ДОО оставляет за собой право в целях обеспечения безопасности электронной системы производить выборочные и полные проверки всей электронной системы и отдельных файлов без предварительного уведомления работников.

7.2. После утверждения настоящего Регламента все пользователи ДОО под личную роспись знакомятся с Регламентом.

УТВЕРЖДАЮ

Заведующий МБДОУ
детского сада № 27

« 24 » 05 2020 г.

Н.И. Кайшева



Регламент работы с электронной почтой

1. Общие положения

1.1. Настоящий Регламент регулирует условия и порядок использования электронной почты в сети Интернет через ресурсы учреждения педагогами и сотрудниками МБДОУ детский сад №27 (далее ДОУ).

1.2. Использование электронной почты в ДОУ направлено на решение задач учебно-воспитательного процесса.

1.3. Настоящий Регламент имеет статус локального нормативного акта учреждения.

1.4. Использование электронной почты в сети Интернет возможно при условии ознакомления лица, пользующегося сетью Интернет в ДОУ, с Регламентом организации доступа к сети Интернет и настоящим Регламентом.

2. Порядок обработки, передачи и приема документов по электронной почте

2.1. По электронной почте производится получение и отправка информации законодательного, нормативно-правового, учебного, учебно-методического характера в учреждения образования и органы управления образованием муниципального образования, других субъектов РФ, а также ближнего и дальнего зарубежья.

2.2. Для обработки, передачи и приема информации по электронной почте в ДОУ приказом заведующей назначается ответственное лицо.

2.3. Ответственное лицо направляет адрес электронной почты образовательного учреждения в орган управления образования муниципалитета. В дальнейшем данного ответственного лица сообщает о любых изменениях адреса электронной почты учреждения.

2.4. Все передаваемые по электронной почте файлы должны пройти проверку антивирусными средствами. Ответственность за ненадлежащую подготовку информации к передаче по электронной почте несет отправитель электронного сообщения.

2.4. Ответственное лицо обеспечивает бесперебойное функционирование электронной почты в течение всего рабочего времени.

2.5. Передаваемая и принимаемая в адрес образовательного учреждения электронная корреспонденция регистрируется в соответствии с правилами делопроизводства, установленными в ДОУ.

2.6. Для отправки электронного сообщения пользователь оформляет документ в соответствии с требованиями, предъявляемыми к оформлению официальных документов, в электронном виде.

2.7. Принятые и отправленные электронные сообщения сохраняются на жестком диске компьютера в соответствующих архивных папках.

2.8. При получении важных писем, требующих подтверждения ответа, ответственное лицо обязано отправить такое подтверждение. Ответственное лицо должно принять меры для

лицо обязано отправить такое подтверждение. Ответственное лицо должно принять меры для обеспечения правильной настройки почтового клиента для возможности отправки подтверждения получения писем в штатном режиме.

2.9. При отправке важных писем в сообщении должна быть указана необходимость подтверждения получения письма адресатом.

2.10. Перед отправлением сообщения необходимо проверять правописание и грамматику текста сообщения. Тексты большого объема желательно отправлять в виде вложения.

2.11. Электронные письма подписываются лицом, производившим отправку корреспонденции. Необходимо настроить почтовый клиент для автоматической вставки подписи в почтовые отправления. Подпись должна содержать: имя, отчество и фамилию отправителя, должность, название образовательного учреждения, название города и края проживания (или другого наименования населенного пункта), контактного телефона отправителя.

2.12. При получении «спама» ответственное лицо обязано сразу удалить такие письма, не открывая вложение (желательно добавить отправителя в список заблокированных отправителей).

2.13. Не удалять входящие и исходящие письма в течение учебного года. В дальнейшем, во избежание переполнения электронного ящика, неактуальные письма подлежат удалению.

2.14. Сформировать структуру папок для упорядочения входящих сообщений. Все передаваемые по электронной почте вложения (файлы) должны быть предварительно проверены антивирусными средствами. Ответственность за ненадлежащую подготовку информации к передаче по электронной почте несет лицо, ответственное за работу с электронной почтой.

2.15. Передаваемые с помощью электронной почты официальные документы должны иметь соответствующие реквизиты (исходящий регистрационный номер, номер и дату приказа, распоряжения и т.п.). В тексте сообщения необходимо обязательно указывать реквизиты и название пересылаемого во вложении официального документа. Передаваемая и принимаемая в адрес образовательного учреждения официальная электронная корреспонденция регистрируется в соответствии с правилами делопроизводства, установленными в образовательном учреждении.

2.16. Все передаваемые учебно-методические и справочно-информационные материалы должны пересылаться с сопроводительным письмом.

2.17. При получении электронного сообщения ответственное лицо:

- регистрирует его в установленном порядке;
- определяет получателя письма (руководитель учреждения, заместители руководителя, бухгалтерия и т.п.) и передает ему документ на рассмотрение. В случае, если получателя корреспонденции ответственному лицу сложно определить самостоятельно, сообщение передаётся руководителю учреждения или одному из его заместителей. Если письмо содержит поясняющий текст к вложению, его необходимо также передать адресату вместе с вложением (распечатанным или в электронном виде);
- в случае невозможности прочтения электронного сообщения, уведомляет об этом отправителя.

3. Порядок обработки, передачи и приема документов по электронной почте в образовательных целях.

3.1. Для получения возможности работы с электронной почтой педагогическим

работникам ДООУ необходимо обратиться с разрешением к лицу, назначенному ответственным за организацию работы сети Интернет в ДООУ.

3.2. По разрешению лица, ответственного за организацию сети и ограничение доступа, педагогические работники получают доступ к компьютеру, подключенному к сети Интернет, после чего ответственный за работу в сети Интернет перекладывается на него.

3.3. Для работы с электронной почтой педагогические работники используют свой личный почтовый ящик. Доступ к почтовому ящику осуществляется с помощью браузера.

3.4. При ведении электронной переписки персональные данные воспитанников (включая фамилию и имя, группу, возраст, фотографии, данные о месте жительства, телефонах и прочее, иные сведения личного характера) могут передаваться только с письменного согласия родителей или иных законных представителей воспитанников.

3.5. В электронных письмах без получения согласия упомянутых лиц или их законных представителей, могут быть указаны лишь фамилия и имя воспитанника, либо фамилия имя и отчество педагога, сотрудника или родителя.

3.6. При получении согласия на передачу персональных данных представитель ДООУ обязан разъяснить возможные риски и последствия их опубликования. ДООУ не несет ответственность за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на передачу персональных данных.

3.8. При отправке сообщения необходимо соблюдать правила этики деловой переписки.

3.9. Все передаваемые учебно-методические и справочно-информационные материалы должны передаваться с сопроводительным письмом.

4. Заключительные положения

- 4.1. Изменения и настоящий Регламент могут вноситься Учреждением в соответствии с действующим законодательством и Уставом ДООУ.
- 4.2. Настоящий Регламент принят на заседании Совета по вопросам регламентации доступа к информации к сети Интернет в установленном порядке.

ПАМЯТКА ПО РАБОТЕ С КОРПОРАТИВНОЙ ЭЛЕКТРОННОЙ ПОЧТОЙ

Политика использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности МПР России и неотделима от нее.

Электронная почта является собственностью МПР России и может быть использована **ТОЛЬКО** в служебных целях. Использование электронной почты в других целях категорически запрещено.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

При работе с корпоративной системой электронной почты сотрудникам МПР России запрещается:

использовать адрес корпоративной почты для оформления подписок;

публиковать свой адрес либо адреса других сотрудников МПР России на общедоступных Интернет-ресурсах (форумы, конференции и т.п.);

открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;

осуществлять массовую рассылку почтовых сообщений рекламного характера;

рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;

распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

распространять информацию, содержание и направленность которой запрещены международным и российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;

распространять информацию ограниченного доступа, предназначенную для служебного использования;

предоставлять кому бы то ни было пароль доступа к своему почтовому ящику.

С настоящей памяткой ознакомлен

_____ (_____)
(подпись) (Ф.И.О.)
"__" _____ 20__ г.

Лист ознакомления с Регламентом работы с электронной почтой в муниципальном дошкольном образовательном учреждении

№	Ф.И.О.	Должность	Дата ознакомления	Подпись

УТВЕРЖДАЮ
Заведующий МБДОУ
детского сада № 27
2020 г.
Н.И.Кайшева



Требования к оборудованию помещений и размещению технических средств, используемых для обработки персональных данных

- Настоящие Требования определяют порядок оборудования выделенных помещений и условия размещения в них технических средств (персональных компьютеров, серверов и т.п.), используемых для обработки персональных данных в МБДОУ детском саду № 27
- Расположение выделенных помещений и размещаемых в них технических средств должно исключать возможность бесконтрольного проникновения в эти зоны посторонних лиц и гарантировать сохранность находящихся в них конфиденциальных документов, содержащих персональные данные.
- Размещение оборудования и технических средств, предназначенных для обработки персональных данных, должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.
- Внутренняя планировка и расположение рабочих мест в выделенных помещениях должны обеспечивать исполнителям сохранность доверенных им конфиденциальных документов и сведений, содержащих персональные данные.
- Входные двери выделенных помещений должны быть оборудованы замками, гарантирующими санкционированный доступ в них в нерабочее время.
- Окна и двери выделенных помещений должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за всеми сигнальными устройствами.
- В выделенные помещения по утвержденному списку допускаются руководство организации, сотрудники службы (ответственный за) информационной безопасности, сотрудники информационно-технической службы, иные уполномоченные лица и исполнители, имеющие прямое отношение к приему, обработке и передаче персональных данных.
- Допуск в выделенные помещения вспомогательного и обслуживающего персонала (уборщицы, электромонтеры, сантехники и т.д.) производится только при служебной

необходимости и в сопровождении ответственного за помещение, при этом необходимо принять меры, исключающие визуальный просмотр конфиденциальных документов, содержащих персональные данные.

- По окончании рабочего дня выделенные помещения необходимо закрывать и опечатывать, затем их сдают под охрану с указанием времени приема/сдачи и отметкой о включении и выключении охранной сигнализации в журнале приема/сдачи помещений под охрану.
- Сдачу ключей и выделенных помещений под охрану, а также получение ключей и вскрытие выделенных помещений имеют право производить только сотрудники, работающие в этих помещениях и внесенные в утвержденный руководством организации список с образцами подписей этих сотрудников. Список хранится у ответственного дежурного подразделения безопасности.
- Перед вскрытием выделенных помещений должна быть проверена целостность оттисков печатей и исправность замков. При обнаружении нарушения целостности оттисков печатей, повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно информируется руководство организации и подразделение безопасности (или иное уполномоченное лицо).
- В случае утраты ключа от входной двери выделенного помещения немедленно ставится в известность подразделение безопасности (или иное уполномоченное лицо).
- В выделенных помещениях, где установлены средства защиты информации от утечки по техническим каналам, запрещается приносить и использовать радиотелефоны/сотовые телефоны и другую радиоаппаратуру.
- На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством организации, в которых предусматривается вызов администрации, должностных лиц, вскрытие выделенных помещений, очередность и порядок спасения конфиденциальных документов, содержащих персональные данные, и дальнейшего их хранения.