АДМИНИСТРАЦИЯ МИХАЙЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА ПРИМОРСКОГО КРАЯ

П О С Т А Н О В Л Е Н И Е

14.04.2025 с. Михайловка № 541-па

Об обеспечении доступа к сети Интернет сотрудников администрации Михайловского муниципального округа

В соответствии с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», в связи с введением в эксплуатацию информационной инфраструктуры в здании администрации Михайловского муниципального округа, подключением сети Интернет через специальные оптико-волоконные линии (ВОЛС) и обеспечение безопасности доступа к сети Интернет через межсетевой экран, а также в целях повышения информационной обеспеченности, внедрения системы электронного документооборота (СЭД), руководствуясь Уставом Михайловского муниципального округа, администрация Михайловского муниципального округа

ПОСТАНОВЛЯЕТ:

1. Муниципальному казённому учреждению Михайловского муниципального округа Приморского края «Учреждение хозяйственного обеспечения» далее – МКУ ММО «УХО» (Корж С.Г.):

1.1. Подключить автоматизированные рабочие места (АРМ), имеющие права доступа к локальной сети администрации округа и сети Интернет согласно Заявки на доступ к информационным ресурсам (Приложение № 1)

1.2. Подключить рабочие места сотрудников администрации округа к сети Интернет согласно принятых заявок на доступ к информационным ресурсам АММО и зарегистрированных в базе пользователей на сетевом оборудовании межсетевого экранирования и имеющих права доступа к локальной сети администрации Михайловского муниципального округа и сети Интернет.

1.3. Укомплектовать помещение серверной дополнительным сетевым оборудованием, обеспечивающим бесперебойную работу информационной инфраструктуры.

2.Утвердить:

2.1. Регламент по администрированию и использованию информационной инфраструктуры администрации Михайловского муниципального округа и сети Интернет (Приложение № 2);

2.2. Регламент работы с электронной почтой в администрации Михайловского муниципального округа (Приложение № 3);

2.3. Регламент использования сотрудниками администрации Михайловского муниципального округа ресурсов глобальной сети Интернет (Приложение № 4);

2.4. Положение по информационной безопасности при работе на персональных компьютерах в информационной инфраструктуре администрации Михайловского муниципального округа (Приложение № 5).

3. Общему отделу администрации округа (Агальцова Н.В.) ознакомить сотрудников администрации под роспись с документами, указанными в пп. 1.2- 2.4.

4. Руководителям структурных подразделений администрации округа обеспечить изучение регламентов работы, указанных в пп. 1.2-2.4 настоящего постановления и осуществлять систематический контроль за их исполнением.

5. Отделу информатизации и информационной безопасности обнародовать настоящее постановление в местах, установленных Уставом

Михайловского муниципального округа.

6. Отделу по культуре, внутренней и молодежной политике (Чаус М.В.) обеспечить публикацию настоящего постановления в общественно-политической газете «Вперед» Михайловского муниципального округа.

7. Контроль за исполнением настоящего постановления возложить на первого заместителя главы администрации округа Н.Н. Мельничук.

И.о. главы Михайловского муниципального округа -
главы администрации округа Н.Н. Мельничук

Приложение № 1
к постановлению администрации
Михайловского муниципального округа
Приморского края
от 14.04.2025 № 541-па

Директору МКУ
ММО ПК «УХО»
_____

ЗАЯВКА

на предоставление доступа АРМ специалиста

к информационным ресурсам АММО

Структурное подразделение
_____

просит разрешить доступ (*ФИО специалиста полностью*)
_____с ПК, зарегистрированного в локальной сети Администрации под IP адресом (заполняется **системным администратором**) _____.

Обоснованием необходимости доступа является следующее:
_____
_

Указывается список ресурсов, к которым необходим доступ*:
_____
_____
_____
_____
_____
_____

Указываются ресурсы такие как сеть Интернет, локальная сеть, локальная папка, СПС Консультант+, электронная почта, учетная запись в CommFort, 1С и др. информационные ресурсы.

Сотрудник

_____

дата подпись

Ф.И.О.

Руководитель структурного подразделения

_____

дата подпись

Ф.И.О.

Приложение № 2

к постановлению администрации
Михайловского муниципального округа
Приморского края
от 14.04.2025 № 541-па

РЕГЛАМЕНТ ПО АДМИНИСТРИРОВАНИЮ И ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ АДМИНИСТРАЦИИ МИХАЙЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА И СЕТИ ИНТЕРНЕТ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент разработан в целях систематизации мероприятий по обслуживанию и использованию информационной инфраструктуры (далее - Локальной сети) и сети Интернет в администрации Михайловского муниципального округа (далее - Администрации) и определяет порядок работы с этими сетями сотрудников администрации и других лиц.

1.2. Ознакомление с Регламентом и его соблюдение обязательны для всех сотрудников, а также иных лиц, допускаемых к работе с сетями в данной организации.

1.3. Настоящий Регламент имеет статус локального нормативного акта Администрации. Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящим Регламентом, применяются нормы действующего законодательства.

2. ОТВЕТСТВЕННЫЕ ЛИЦА

2.1. Ответственные сотрудники за настройку Локальной сети, за настройку сети Интернет, за контроль над использованием сетей назначаются приказами Муниципального казенного учреждения Михайловского муниципального округа Приморского края «Учреждения хозяйственного обеспечения», в ведении которого находятся Локальные сети и оборудование для обеспечения работоспособности Локальной сети Администрации.

3. ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ СЕТЕЙ

3.1. Подключение оборудования и настройку Локальной сети в Администрации производят ответственные сотрудники за настройку

соответствующих сетей. Другим лицам запрещается осуществлять попытки подключения оборудования и настройки сети.

3.2. При необходимости участие внешних организаций в подключении оборудования и настройке сетей допускается с разрешения директора МКУ ММО «УХО» и системного администратора организации.

4. ПРАВИЛА ИСПОЛЬЗОВАНИЯ СЕТЕЙ

4.1. Использование Локальной сети допускается только в целях, непосредственно связанных с рабочими задачами и рабочим процессом.

4.2. Доступ к ресурсам, несовместимым с целями и задачами рабочего процесса, запрещён.

4.3. При использовании ресурсов Локальной сети обязательным является соблюдение законодательства об интеллектуальных правах и иного применимого законодательства.

4.4. Сотрудники Администрации, имеющие рабочее место, оборудованное компьютером с подключением к Локальной сети, используют сеть в любое время в рамках режима работы учреждения.

4.5. Для предотвращения доступа к запрещенным ресурсам используются меры дисциплинарного характера, специализированное программное обеспечение (межсетевой экран). По каждому выявленному факту доступа к таким ресурсам ответственным сотрудником по контролю за использованием сетей составляется докладная записка на имя руководителя. Ответственность за последствия доступа к нежелательным ресурсам несёт лицо, осуществившее доступ к этим ресурсам.

4.6. При использовании сетевых сервисов, предполагающих авторизацию, запрещается пользоваться чужими учётными данными.

Все компьютеры, подключаемые к любой из сетей, обязаны иметь установленное, действующее и обновляющееся антивирусное программное обеспечение.

4.7. По решению системного администратора совместно с руководителем подразделения, в котором работает сотрудник, может быть лишен права пользования сетями (как временно, так и постоянно) за неоднократные нарушения настоящего Регламента. Такое решение может быть отменено только руководителем.

4.8. Запрещено самовольно пытаться подключаться к Локальной сети Администрации, пытаться вскрывать сетевое оборудование и производить сетевые настройки компьютера, подключенного к Локальной сети Администрации. Все действия по настройке, подключению производить только по согласованию с системным администратором Администрации.

4.9. К сетевому оборудованию в кабинетах следует относиться бережно, исключать сильное термическое и физическое воздействие на узлы сетевой инфраструктуры. В коридорах и местах общего пользования, где имеется кабель-трассы локальной сети, запрещается вскрывать кабель-каналы. В случае обнаружения вскрытого кабель-канала локальной сети, необходимо незамедлительно сообщить об этом руководителю и системному

администратору Администрации. Следует помнить, что любое повреждение сетевого кабеля в кабель-трассах приведет к прекращению функционирования конечного разъема в кабинете и потребует полной замены кабеля от серверного помещения до конечного устройства локальной сети.

5. ДЕЙСТВИЯ В НЕШТАТНЫХ СИТУАЦИЯХ

5.1. При утрате (в том числе частично) работоспособности Локальной сети или сети Интернет лицо, обнаружившее неисправность, сообщает об этом ответственному сотруднику или системному администратору. Системный администратор устраняет неисправность, а при отсутствии такой возможности ставит в известность своего руководителя. Руководитель организует устранение неисправности - возможно, с привлечением сил и средств окружных служб или сторонних организаций.

5.2. При прекращении работы сети Интернет во всём учреждении системный администратор проверяет исправность Локальной сети администрации, подключений оборудования и настроек сети. В случае их исправности системный администратор ставит в известность руководителя и связывается с поставщиком услуг сети Интернет.

5.3. При заражении компьютера вирусами его использование немедленно прекращается сотрудником, обнаружившим заражение. О сложившейся ситуации сообщается системному администратору. Компьютер отключается от сетей до момента очистки от всех вирусов. Разрешение на дальнейшее использование компьютера и подключение его к сетям даёт системный администратор после соответствующей проверки.

6. РЕГЛАМЕНТНЫЕ РАБОТЫ ПО ОБСЛУЖИВАНИЮ ЛОКАЛЬНЫХ СЕТЕЙ

6.1. Регламентные работы по обслуживанию сетевого оборудования проводятся в строго отведенное время. Работы проводятся с целью профилактики оборудования, выявления проблем в работе сетевого оборудования и предотвращения внештатных ситуаций в работе локальной сети и услуг сети Интернет.

6.2. Регламентные работы должны проводиться во внерабочее время, исключения составляют работы при возникновении внештатных ситуаций.

6.3. График работ предусматривает ежедневный контроль и осмотр сетевого оборудования в серверном помещении. Регламентные работы включают в себя мероприятия по настройке серверного оборудования, плановые перезагрузки серверов, маршрутизаторов и прочего сетевого оборудования.

7. АДМИНИСТРИРОВАНИЕ ДОСТУПА К СЕТИ ИНТЕРНЕТ

7.1. Администрирование доступа к сети Интернет производится через межсетевой экран, который установлен в серверном помещении и работает в серверном шкафу.

7.2. Доступ в серверное помещение и к серверному оборудованию ограничен. Доступ к серверному оборудованию имеет только системный администратор.

7.3. Межсетевой экран устанавливается на границе Локальной сети Администрации и глобальной сети Интернет. Межсетевой экран обеспечивает защиту Локальной сети Администрации от сетевых атак, вредоносного контента, также позволяет разграничить доступ к тем или иным Интернет-ресурсам, производить мониторинг пользователей, имеющих доступ к сети Интернет.

7.4. Доступ к сети Интернет производится посредством авторизации рабочего компьютера на межсетевом экране через присвоенный IP адрес локальному компьютеру. Перечень запрещенных ресурсов и контента, а также порядок работы в сети Интернет расписаны в Регламенте использования работниками администрации Михайловского муниципального округа ресурсов глобальной сети Интернет (Приложение № 5 к постановлению администрации Михайловского муниципального округа).

7.5. Администрирование доступа к сети Интернет производится только с компьютера системного администратора и только под учетной записью главного администратора через web-интерфейс межсетевой экрана с применением парольной защиты. С другого рабочего места доступ к настройкам межсетевого экрана заблокирован.

Приложение № 3
к постановлению администрации
Михайловского муниципального округа
Приморского края
от 14.04.2025 № 541-па

РЕГЛАМЕНТ
РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ В АДМИНИСТРАЦИИ МИХАЙЛОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

1. Общие положения

1.1. Настоящий регламент определяет порядок ведения открытой служебной переписки в администрации Михайловского муниципального округа (далее- Администрации) по электронной почте.

По электронной почте производится направление в исполнительные органы государственной власти Приморского края, органы местного самоуправления, территориальные органы федеральных органов исполнительной власти и другие организации (далее - Подразделения):

планов работы Администрации;

правовых актов главы Администрации;

методической и справочной информации;

запросов на представление оперативной информации;

приглашений на совещания;

других информационно-справочных документов.

Допускается рассылка служебных писем, нормативных актов Администрации, как неофициальных электронных копий с последующим направлением копий на бумажном носителе.

Официальным адресом электронной почты Администрации является адрес: priemnaya@mikhprim.ru Электронная корреспонденция, полученная/отправленная с этого адреса, обрабатывается в общем отделе Администрации.

Служебная электронная почта является собственностью Администрации и может быть использована ТОЛЬКО в служебных целях. Использование электронной почты в других целях категорически запрещено.

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

Официальные адреса электронной почты структурных подразделений, сотрудников Администрации определяются их руководителями.

Для обработки, передачи и приема информации по электронной почте в структурных подразделениях Администрации назначается ответственное лицо.

Ответственное лицо направляет адрес электронной почты

подразделения, сотрудников системному администратору для формирования единой адресной книги. В дальнейшем данное ответственное лицо сообщает о любых изменениях адресов электронной почты системному администратору.

Удаленные структурные подразделения должны обеспечить бесперебойное функционирование электронной почты.

Все передаваемые по электронной почте файлы должны пройти антивирусную проверку. Ответственность за ненадлежащую подготовку информации к передаче по электронной почте несёт ответственное лицо.

Передаваемые с помощью электронной почты официальные документы должны иметь подлинник документа на бумажной основе.

Электронные копии справочно-информационных материалов, не имеющие исходящего регистрационного номера, при отправлении электронной почтой могут не иметь бумажной копии и должны передаваться с сопроводительным письмом, подписанным должностным лицом.

Порядок обработки, передачи и приема документов по электронной почте

Передаваемая и принимаемая в адрес Администрации электронная корреспонденция регистрируется в общем отделе в соответствии с Инструкцией по делопроизводству в администрации Михайловского муниципального округа.

2.2. Для отправки электронного сообщения исполнитель оформляет документ в соответствии с требованиями, предъявляемыми к оформлению официальных документов, и представляет оригинал вместе с электронной копией документа на съёмных носителях в общий отдел Администрации и(или) ответственному лицу в структурном подразделении.

2.3. Общий отдел или ответственное лицо отправляет документ адресату. После отправки электронная копия на съёмном носителе возвращается исполнителю.

2.4. При отправлении файлов с сопроводительным письмом оно регистрируется в установленном порядке и вместе с файлами передается адресату.

2.5. При получении электронного сообщения ответственное лицо:

- распечатывает полученное электронное сообщение в 1 экземпляре, регистрирует в установленном порядке;

- передает документ на бумажной основе на рассмотрение руководителю или, если указано, непосредственно адресату;

- в случае невозможности прочтения электронного сообщения уведомляет об этом отправителя, системного администратора.

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

2.7. Порядок регистрации электронной корреспонденции в структурных подразделениях Администрации определяется их руководителями.

3. Ограничения при работе с электронной почтой.

3.1. При работе со служебной системой электронной почты сотрудникам Администрации ЗАПРЕЩАЕТСЯ:

3.1.1. публиковать свой адрес электронной почты либо адреса других сотрудников Администрации на общедоступных Интернет- ресурсах (форумы, конференции и т.п.) за исключением случаев служебной необходимости

3.1.2. использовать адрес электронной почты для оформления подписок

3.1.3. осуществлять массовую рассылку почтовых сообщений рекламного характера;

3.1.4. 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;

3.1.5. 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;

3.1.6. распространять информацию, содержание и направленность которой запрещены международным и российским законодательством, включая материалы, несущие:

- вредоносную, угрожающую, клеветническую, непристойную информацию;
- оскорбляющую честь и достоинство других лиц;
- способствующую разжиганию национальной розни, подстрекающую к насилию и призывающую к совершению противоправной деятельности, в том числе разъясняющую порядок применения взрывчатых веществ и иного оружия.

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

Приложение № 4
к постановлению администрации
Михайловского муниципального округа
Приморского края
от 14.04.2025 № 541-па

РЕГЛАМЕНТ
использования сотрудниками администрации Михайловского муниципального округа ресурсов глобальной сети Интернет

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Регламент использования сотрудниками администрации Михайловского муниципального округа (далее - Администрация) доступа к сети Интернет (далее- Регламент) регулирует условия и порядок использования сети Интернет в Администрации.

1.2. Регламент распространяется на сотрудников Администрации, выполнение должностных обязанностей которых связано с использованием персональных компьютеров, подключённых к сети Интернет (далее- Пользователи), и определяет их полномочия, обязанности и ответственность при использовании сети Интернет.

1.3. Регламент является обязательным для выполнения всеми Пользователями Администрации.

1.4. Использование сети Интернет в Администрации осуществляется в целях повышения эффективности работы сотрудников, внедрения электронного документооборота, координации и взаимодействия территориальных отделов округа.

2. Назначение доступа к ресурсам сети Интернет

2.1. Доступ к ресурсам сети Интернет предоставляется сотрудникам для выполнения ими прямых должностных обязанностей.

2.2. Глобальная информационная сеть Интернет используется для:

2.2.1. доступа к мировой системе гипертекстовых страниц (www);

2.2.2. доступа к файловым ресурсам Интернета, локальной сети администрации (FTP);

2.2.3. доступа к специализированным (правовым и др.) базам данных;

2.2.4. контактов с органами государственной, региональной и муниципальной власти, с сотрудниками структурных подразделений Администрации;

2.2.5. обмена электронной почтой с официальными лицами по не конфиденциальным вопросам административного характера;

2.2.6. повышения квалификации сотрудников, необходимой для выполнения сотрудником своих должностных обязанностей;

2.2.7. поиска и сбора информации по управленческим, административным, финансовым, юридическим вопросам, если эти вопросы напрямую связаны с выполнением сотрудником его должностных обязанностей;

2.2.8. другие цели.

3. Доступ к Интернет-ресурсам

3.1. Администрация обеспечивает доступ Пользователей к ресурсам сети Интернет по специальным каналам связи в соответствии с настоящим Регламентом.

3.2. Без согласования с руководителем структурного подразделения, в котором работает сотрудник, и системным администратором запрещена самостоятельная организация дополнительных точек доступа в Интернет (удаленный доступ, канал по локальной сети и пр.).

4. Регистрация Пользователя

4.1. Доступ к сети Интернет осуществляется с рабочего персонального компьютера Пользователя.

4.2. Каждому подключенному к сети Интернет персональному компьютеру назначается Пользователь, ответственный за данный компьютер.

4.3. Пользователю присваиваются идентификационный номер, IP-адрес и пароль (далее - Сетевые данные)

4.4. Информация о Пользователе, его Сетевые данные и идентификационные данные персонального компьютера, заносятся в базу данных Пользователей Администрации и хранятся в базе межсетевого экрана.

4.5. Пользователь обязан хранить Сетевые данные и идентификационные данные компьютера в тайне. Запрещена передача этой информации третьим лицам. За все деструктивные действия, произведённые в сети, отвечает Пользователь. При подозрении на то, что Сетевые данные стали известны третьим лицам, Пользователь обязан немедленно обратиться к системному администратору с целью их изменения.

4.6. Временное ограничение права доступа Пользователя к сети Интернет возможно только по основаниям, установленным в Положении об информационной безопасности Администрации.

5. Ограничения при работе в сети Интернет

5.1. Пользователю запрещается самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения.

5.2. Пользователю запрещено производить какие-либо действия с информацией, заражённой вирусом.

5.3. Пользователю запрещается единовременно скачивать большой объём информации, значительно увеличивающий нагрузку сети и мешающий нормальной работе других Пользователей.

5.4. Пользователю запрещён доступ к следующим ресурсам сети Интернет:

- националистического характера;
- призывающим к насилию и терроризму;
- эротического и порнографического характера;
- социальным сетям, если это не входит в должностные обязанности, сохранение их контента на рабочий компьютер (Одноклассники, Вконтакте, Мой Мир и пр.)
- игровым, развлекательным и прочим ресурсам, не имеющим отношения к деятельности Администрации и исполнению Пользователем должностных обязанностей.

5.5. Пользователю запрещается совершать следующие действия в личных целях:

- использовать электронную почту;
- размещать информацию на досках объявлений в сети Интернет;
- участвовать в форумах и конференциях, проводимых в сети Интернет;
- просматривать и прослушивать видео- и аудио-, ТВ - и музыкальные программы, транслируемые в сети Интернет;
- размещать информацию о поисках работы и просматривать информацию о вакансиях.
- размещать публикацию служебного электронного адреса на досках объявлений, в конференциях и гостевых книгах;
- использовать некорпоративные e-mail адреса для рассылки служебной информации;

5.6. Пользователю запрещается копировать и использовать материалы, защищённые законодательством об авторских правах.

6. Время работы Пользователей в сети Интернет

6.1. Время работы Пользователей в сети Интернет ограничено. Доступ к сети Интернет предоставляется согласно режиму работы Администрации;

6.2. В случае необходимости использования сети Интернет в выходные дни или по окончанию времени, указанного в пункте 6.1 Регламента, Пользователь обязан получить разрешение руководителя структурного подразделения и уведомить системного администратора о необходимости снятия ограничения для данного Пользователя.

7. Контроль использования ресурсов сети Интернет

7.1. Администрация оставляет за собой право в целях обеспечения политики информационной безопасности производить выборочные и полные

проверки сетевых ресурсов и отдельных файлов без предварительного уведомления сотрудников.

7.2. Системный администратор, используя программное обеспечение, осуществляет контроль за соблюдением настоящего Регламента.

7.3. После утверждения настоящего Регламента все сотрудники Администрации под личную роспись знакомятся с Регламентом.

Приложение № 5
к постановлению администрации
Михайловского муниципального округа
Приморского края
от 14.04.2025 № 541-па

Положение
по информационной безопасности при работе на персональных компьютерах в информационной инфраструктуре администрации Михайловского муниципального округа

1. **Общие положения.**

1.1. Целью настоящего Положения является определение основных требований, обязательных для исполнения при работе на персональных компьютерах (ПК) в информационной инфраструктуре (локальной сети) администрации Михайловского муниципального округа (Администрации).

1.2. Положение распространяется на выполнение любых работ посредством ПК.

1.3. Работники Администрации и лица, не работающие в Администрации (в дальнейшем - пользователи) допускаются к работе на ПК только после ознакомления с настоящим Положением под роспись. Ответственность за ознакомление с Положением несет руководитель подразделения, в котором осуществляется работа на ПК.

1.4. Контроль за исполнением требований настоящего Положения возлагается:

"по Администрации в целом - специалист по информационной безопасности (ИБ);

"по работе на персональных компьютерах Администрации, установленному программному обеспечению - на системного администратора Администрации;

"по работе с Интернетом, электронной почтой - на системного администратора Администрации.

2. Требования к ПК в Администрации.

2.1. ПК в Администрации должны удовлетворять следующим требованиям:

2.1.1. Все ПК должны быть подключены к локальной сети Администрации;

2.1.2. Отсутствуют или отключено аппаратное и программное обеспечение для передачи данных, минуя локальную сеть;

2.1.3. Отсутствуют или отключены устройства для работы со сменными носителями информации (дисководы гибких дисков, CD ROM, Flash - носители) если этого требует режим работы конкретного специалиста подразделения;

2.1.4. Опечатан системный блок;

2.1.5. Имеется паспорт компьютера, подписанный ответственным сотрудником, с перечисленными в нем техническими характеристиками, установленным системным программным обеспечением;

2.1.6. Имеется список пользователей ПК, допущенных к работе с указанием ответственного за эксплуатацию данного ПК;

2.1.7. Установлено антивирусное программное обеспечение. Обновление антивирусных баз не реже "N" раз в неделю;

2.1.8. Вход в BIOS закрыт паролем. Отключена загрузка ПК с внешних носителей (FDD, CD, LAN, ...);

2.1.9. Смена пароля пользователя на доступ к ПК должна производится не реже 1 раза в 3 месяца, для администраторов не реже 1 раза в месяц;

2.1.10. Для ПК файловая система основного раздела должна быть NTFS;

2.1.11. Папка для обмена информацией по локальной сети должна быть доступна на запись для файловых систем FAT, для систем NTFS - только на «Запись» и «Чтение содержимого папки». При наличии на ПК диска с файловой системой NTFS папка для обмена должна располагаться только на этом диске.

3. Порядок предоставления прав доступа к ПК, ресурсам и программам локальной сети Администрации.

3.1. Предоставление сотрудникам Администрации прав доступа к необходимым для работы программам выполняется по заявке руководителя структурного подразделения (Приложение 1). При изменении состава программного обеспечения (замена, первоначальная установка) начальник структурного подразделения направляет системному администратору служебную записку на согласование и проведение мероприятий по заявленным в служебной записке действиям.

3.2. Предоставление лицам, не работающим в Администрации, прав доступа к автоматизированным рабочим местам сотрудников запрещено.

3.3. Руководитель структурного подразделения своим распоряжением определяет перечень сотрудников подразделения, имеющих доступ к каждому конкретному ПК.

3.4. Постоянный доступ к сети Интернет и личным почтовым ящикам предоставляется по письменному разрешению начальника структурного подразделения по согласованию с системным администратором.

4. Пользователям запрещается:

4.1. использовать компоненты программного и аппаратного обеспечения в неслужебных целях;

4.2. посещать в интернет-сайты, содержащие информацию, не входящую в круг служебных обязанностей сотрудника;

4.3. получать и отправлять по электронной почте программное обеспечение без согласования с системным администратором;

4.4. изменять параметры сетевой идентификации компьютера (имя, IP адрес);

4.5. предоставлять права удаленного доступа к системным ресурсам своего ПК (корневой раздел жесткого диска, на котором установлена операционная система, каталоги, в которых установлена операционная система);

4.6. самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые системные программные и аппаратные средства, не предусмотренные паспортом ПК;

4.7. отключать свой ПК от локальной сети без согласования с системным администратором;

4.8. снимать пломбу с компьютера;

4.9. предоставлять закреплённый за ними ПК в пользование другим лицам или сотрудникам, не имеющим права доступа согласно настоящему положению за исключением технического обслуживающего персонала;

4.10. записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках и т.п.);

4.11. оставлять включенный без присмотра свой ПК, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

4.12. оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

4.13. использовать и хранить на рабочих местах съемные носители информации (Flash-карты, CD диски и т.п., в том числе цифровые фотокамеры) без специального разрешения;

4.14. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению конфликтной ситуации. Об обнаружении такого рода ошибок ставить в известность ответственного за безопасность информации и руководителя своего подразделения;

4.15. предпринимать попытки взлома компьютерной защиты ПК других пользователей, локальной сети Администрации, ресурсов сторонних организаций;

4.16. предпринимать действия, направленные на несанкционированное получение прав доступа к программам, базам данных и иной информации, хранящейся в локальной сети, на ПК других пользователей;

4.17. сообщать кому бы то ни было, кроме непосредственного руководителя (записывать в доступном месте), свой пароль (пароли);

4.18. посылать в электронном виде информацию, содержащую сведения ограниченного распространения без применения программного обеспечения для ее защиты;

4.19. использовать файлы, полученные по почте, через Интернет или со сменных носителей без предварительной проверки на наличие вирусов;

4.20. получать и использовать удалённый доступ на управление ПК других пользователей и серверов.

4.21. устанавливать, использовать и распространять программное обеспечение в локальной сети без согласования с системным администратором.

5. Действия при возникновении неисправностей.

5.1. В случае неправильной работы программного обеспечения, обнаружении вирусов, технической неисправности ПК ставить в известность системного администратора.

5.2. В случае проблем при работе с Интернет, электронной почтой обращаться к системному администратору.

6. Разграничение ответственности по информационной безопасности.

6.1. Ответственность за безопасность загруженной информации через Интернет и электронную почту, возлагается на пользователя, осуществившего приём этой информации. Если пользователь не выявлен, то ответственность несёт лицо, закреплённое за ПК.;

6.2. Ответственность за информационную безопасность при работе в локальной сети Администрации, установку и обновление сетевого антивирусного программного обеспечения возлагается на специалиста по информационной безопасности.

7. Контроль за соблюдением требований по обеспечению информационной безопасности.

7.1. Контроль за соблюдением требований по обеспечению информационной безопасности осуществляют:

" по работе в локальной сети, установленному системному программному обеспечению, функционированию средств защиты информации - системный администратор совместно со специалистом по информационной безопасности,

" по работе с Интернетом, электронной почтой - системный администратор совместно со специалистом по информационной безопасности.

7.2. Использование сотрудниками ПК, доступа в Интернет и электронной почты может наблюдаться, протоколироваться и периодически проверяться.

7.3. В целях проведения проверок устойчивости компьютерной защиты, соблюдения сотрудниками требований настоящего Положения ответственными сотрудниками, системным администратором совместно со специалистом по информационной безопасности могут проводиться проверочные мероприятия, не нарушающие целостность и работоспособность аппаратно-программных средств.

8. Ответственность.

8.1. За неисполнение требований по информационной безопасности руководители подразделений и пользователи несут административную и дисциплинарную ответственность.

8.2. Ответственность за сохранность пломб, установленных на ПК, несет пользователь ПК. В случае нарушения целостности пломб, системный администратор проводит служебное расследование, с целью выявления нарушения и составления акта.