

ПРИКАЗ

01.10.2018

№ 168

г. Керчь

**Об утверждении регламентов
по безопасному пользованию
ресурсами сети Интернет**

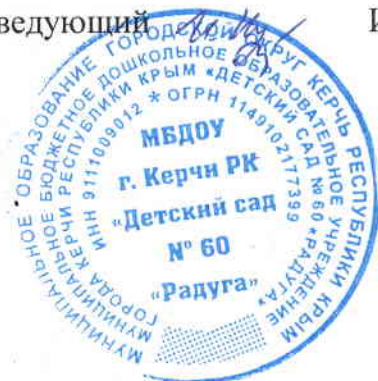
В целях создания условий для эффективного и безопасного использования сети Интернет в решении задач деятельности МБДОУ, в т.ч. организации образовательной деятельности, в соответствии с Федеральным законом «Об образовании в Российской Федерации» от 29.12.2012г. № 273-ФЗ, Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и (или) развитию» (с изменениями и дополнениями), Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (с изменениями),

ПРИКАЗЫВАЮ:

1. Утвердить:
 - 1.1. Регламент № 1 работы с электронной почтой в МБДОУ (*Приложение 1*)
 - 1.2. Регламент № 2 организации антивирусной защиты (*Приложение 2*)
2. Ознакомить работников, имеющими доступ к электронной почте в МБДОУ, с Регламентом № 1 под подпись (*Приложение 3*).
3. Контроль за исполнением данного приказа оставляю за собой.

Заведующий

И.Л. Курилина



Регламент № 1 работы с электронной почтой

1. Общие положения

1. 1. Политика использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности.
1. 2. Электронная почта в МБДОУ г. Керчи РК «Детский сад № 60 «Радуга» (далее – МБДОУ) может использоваться только в служебных целях.
1. 3. По электронной почте производится обмен информацией законодательного, нормативно-правового, учебно-методического характера между МБДОУ и Учредителем, Управлением образования, образовательными организациями, контролирующими, надзорными органами, поставщиками товаров и услуг, подрядчиками и другими организациями, предприятиями и учреждениями, связанными с образовательным учреждением договорными или иными обязательствами (далее – Адресат).
1. 4. Для приема, обработки и передачи информации по электронной почте приказом заведующего назначается ответственное лицо и определяется перечень работников, имеющих доступ к электронной почте МБДОУ (далее – Пользователи). В случае отсутствия ответственного (отпуск, болезнь) – его функции по приказу возлагаются на другого работника МБДОУ
1. 5. Пользователи должны выполнять инструкции, правила по работе с электронной почтой, а также требования данного Регламента.

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

- 2.1. МБДОУ обеспечивает бесперебойное получение и регистрацию электронной почты в течение рабочего дня.
- 2.2. При получении электронного сообщения ответственное лицо:
 - регистрирует его в порядке, установленном Инструкцией МБДОУ по делопроизводству;
 - определяет получателя письма (должностное лицо) и передает ему документ на рассмотрение. В случае если получателя корреспонденции ответственному лицу сложно определить самостоятельно, сообщение передаётся заведующему для вынесения резолюции. Если письмо содержит поясняющий текст к вложению, передает получателю вместе с вложением;
 - в случае невозможности прочтения электронного сообщения уведомляет об этом отправителя.
- 2.3. При получении важных писем, требующих подтверждения ответа, ответственное лицо обязано отправить такое подтверждение. При отправке важных писем, ответственное лицо должно указать в сообщении необходимость подтверждения получения письма Адресатом.
- 2.4. При получении СПАМА (нежелательные электронные письма, как правило, рекламного характера), ответственное лицо обязано сразу удалить такие письма, не открывая вложение (желательно добавить отправителя в список заблокированных отправителей).

- 2.5. Не рекомендуется удалять входящие и исходящие письма в течение учебного года. В дальнейшем, во избежание переполнения электронного ящика старые неактуальные письма необходимо удалить.
- 2.6. При передаче электронной корреспонденции в строке «Тема» указывается краткое содержание послания (заголовок).
- 2.7. Официальные документы передаются в виде прикрепленных файлов с сопроводительным письмом (в тексте необходимо обязательно указывать реквизиты и название пересылаемого во вложении официального документа). Краткая информация просто помещается в текст письма.
- 2.8. При невозможности получения-отправки электронной корреспонденции по любой из причин (отсутствие связи, отсутствие соединения с Интернет, неисправность компьютера, проблемы с используемым программным обеспечением и т.п.) ответственное лицо должно обратиться к руководителю МБДОУ для решения вопроса об устранении проблемы. При невозможности быстрого устранения проблемы, ответственное лицо должно оповестить Адресатов о возникшей проблеме и указать возможные каналы связи.

3. Пользователям запрещено:

- 3.1. Участвовать в рассылке личных сообщений, не связанных с функциональными обязанностями и направлениями деятельности МБДОУ.
- 3.2. Пересылать по произвольным адресам не затребованную потребителями информацию (спам). В случае обнаружения рассылки спама электронные почтовые ящики будут заблокированы до выявления причин и нарушителей.
- 3.3. Электронное послание не должно использоваться для пересылки секретной и конфиденциальной информации.
- 3.4. 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.

Регламент № 2 организации антивирусной защиты

1. Общие положения

1. 1. Целью создания системы антивирусной защиты МБДОУ г. Керчи РК «Детский сад № 60 «Радуга» (далее – МБДОУ) является обеспечение защищенности информационно-коммуникационной системы (далее – ИКС) от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа пользователей МБДОУ к непродуктивным Интернет-ресурсам и контроля их электронной переписки.
1. 2. В МБДОУ заведующим назначается лицо, ответственное за антивирусную защиту.
1. 3. На всех объектах ИКС должно использоваться только лицензионное антивирусное программное обеспечение. Выбор антивирусной программы может производиться как среди коммерческих (платных) программ, так и среди распространяемых бесплатно.
1. 4. Вновь устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

2. Требования к проведению мероприятий по антивирусной защите

2. 1. Обязательному антивирусному контролю подлежит любая информация, получаемая и передаваемая по телекоммуникационным каналам (текстовые файлы любых форматов, файлы данных, исполняемые файлы), а также информация на съемных носителях (оптических, полупроводниковых, магнитных). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
2. 2. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.
2. 3. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.
2. 4. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:
 - после установки (изменения) программного обеспечения компьютера. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение, и лица, ответственного за антивирусную защиту
 - при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках)

2.5. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов лицо, ответственное за антивирусную защиту обязано:

- приостановить работу;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести «лечение» или «уничтожение» (при невозможности «лечения») зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на гибком магнитном диске в организацию, с которой заключен договор на антивирусную поддержку для дальнейшего исследования.