

«СОГЛАСОВАНО»:
Председатель ПК:
Л.В. Динейкина/
«19» апреля 2019 г.

«УТВЕРЖДАЮ»:
Директор МОУ «СОШ №15»:
С.В. Коваленко/
«19» апреля 2019 г.

ПОРЯДОК

организации доступа к информационным ресурсам посредством сети Интернет в образовательной организации

1. Общие положения

Использование сети Интернет в муниципальном общеобразовательном учреждении «Средняя общеобразовательная школа №15» (далее- МОУ «СОШ №15») направлено на решение задач учебно-воспитательного процесса и подчинено следующим принципам:

- соответствия образовательным целям;
- содействия гармоничному формированию и развитию личности;
- уважения закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;
- приобретения новых навыков и знаний;
- расширения применяемого спектра учебных и наглядных пособий;
- социализации личности, введения в информационное общество.

1.2. Использование сети Интернет в образовательном учреждении должно осуществляться в соответствии с:

Конституцией Российской Федерации (Собрание законодательства Российской Федерации, 2009, № 4 ст. 445);

Законом Российской Федерации от 29 декабря 2012 года № 273 «Об образовании»

Постановлением Правительства Российской Федерации от 7 февраля 2011 года № 61 «О федеральной целевой программе развития образования на 2011-2015 годы»;

Федеральным законом от 7 июля 2003 года № 126-ФЗ «О связи»;

Федеральным законом от 7 февраля 1992 года № 2300-1 «О защите прав потребителей»;

Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Постановлением Правительства РФ от 23 января 2006 года №32 «Об утверждении правил оказания услуг связи по передаче данных»;

Постановлением Правительства РФ от 10 сентября 2007 года №575 «Об утверждении правил оказания телематических услуг связи»;

2. Требования к порядку предоставления доступа к сети Интернет

Политика использования сети Интернет.

1. Использование сети Интернет в ОУ возможно исключительно при условии ознакомления и согласия лица, пользующегося сетью Интернет в ОУ, с настоящими Правилами.
2. Руководитель ОУ является ответственным за обеспечение эффективного и безопасного доступа к сети Интернет в ОУ, а также за внедрение соответствующих технических, правовых и иных механизмов в ОУ.
3. Во время занятий контроль за использованием учащимися ресурсов сети Интернет в соответствии с настоящим Правилами осуществляет преподаватель, ведущий занятие.

Преподаватель:

- наблюдает за использованием компьютера и ресурсов сети Интернет учащимися;
- запрещает дальнейшую работу учащегося в сети Интернет в случае нарушения учащимся настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в образовательном учреждении;
- принимает предусмотренные настоящими Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.

Во время использования сети Интернет для свободной работы контроль за использованием сети Интернет осуществляет лицо, уполномоченное на то руководством образовательного учреждения (далее – Уполномоченное лицо).

Уполномоченное лицо:

- определяет время и место для свободной работы в сети Интернет учащихся, преподавателей и сотрудников ОУ с учетом использования соответствующих технических мощностей ОУ в образовательном процессе, а также длительность сеанса работы одного человека;
- контролирует объем трафика ОУ в сети Интернет;
- наблюдает за использованием компьютера и ресурсов сети Интернет учащимися;
- запрещает дальнейшую работу пользователя в сети Интернет в случае нарушения пользователем настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в образовательном учреждении;
- не допускает пользователя к работе в Интернете в предусмотренных настоящими Правилами случаях;
- принимает предусмотренные настоящими Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.

5. При использовании сети Интернет в ОУ осуществляется доступ только на ресурсы, содержание которых не противоречит законодательству Российской Федерации и не является несовместимым с целями и задачами образования и воспитания учащихся.

Проверка такого соответствия осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, имеющихся в ОУ или предоставленного оператором услуг связи (провайдером).

Использование сети Интернет в ОУ без применения данных технических средств и программного обеспечения (например, в случае технического отказа) допускается только для лиц, достигших 18 лет, с индивидуального разрешения Директора ОУ.

6. Принятие решения о политике доступа к ресурсам/группам ресурсов сети Интернет принимается ОУ самостоятельно либо с привлечением внешних экспертов, в качестве которых могут привлекаться:

- преподаватели ОУ и других образовательных учреждений;
- лица, имеющие специальные знания, либо опыт работы в рассматриваемой области;
- представители органов управления образованием;
- родители учащихся.

При принятии решения ОУ, эксперты руководствуются:

- законодательством Российской Федерации;
- специальными знаниями, в том числе, полученными в результате профессиональной деятельности по рассматриваемой тематике;
- интересами учащихся, целями образовательного процесса;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

7. Отнесение определенных категорий и/или ресурсов в соответствующие группы, доступ к которым регулируется техническими средствами и программным обеспечением контентной фильтрации, осуществляется лицом, уполномоченным Директором ОУ.

Категории ресурсов, в соответствии с которыми определяется политика использования сети Интернет в ОУ и доступ к которым регулируется техническими средствами и программным обеспечением контентной фильтрации, определяются в установленном порядке.

8. Принципами размещения информации на Интернет-ресурсах ОУ являются:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защита персональных данных учащихся, преподавателей и сотрудников;
- достоверность и корректность информации.

Персональные данные об учащихся (фамилия и имя, класс, возраст, фотография, место жительства, телефоны и иные контакты, иные сведения личного характера) могут размещаться на Интернет-ресурсах ОУ только с письменного согласия родителей или иных законных представителей учащихся. Персональные данные преподавателей и сотрудников ОУ размещаются на Интернет-ресурсах ОУ только с письменного согласия преподавателя или сотрудника, чьи персональные данные предполагаются к размещению.

В информационных сообщениях о мероприятиях на сайте ОУ и его подразделений без согласия лица или его законного представителя могут быть упомянуты только фамилия и имя учащегося либо фамилия, имя и отчество преподавателя сотрудника родителя.

При истребовании такого согласия представитель ОУ разъясняет лицу возможные риски и последствия опубликования персональных данных. ОУ не несет ответственности в случае наступления таких последствий, если имелось письменное согласие лица (его представителя) на опубликование персональных данных.

Процедура использования сети Интернет

1. Использование сети Интернет в ОУ осуществляется, как правило, в целях образовательного процесса.

2. По разрешению Уполномоченного лица учащиеся (с согласия родителей законных представителей), преподаватели и сотрудники вправе:

- размещать собственную информацию в сети Интернет на Интернет-ресурсах ОУ;
- иметь учетную запись электронной почты на Интернет-ресурсах ОУ.

3. Пользователю запрещается:

- находиться на ресурсах, содержание и тематика которых является недопустимой для несовершеннолетних и/или нарушающей законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризм, политический или религиозный экстремизм, национальная и расовая и т.п. розни; иные ресурсы схожей направленности);
- осуществлять любые коммерческие сделки через Интернет;
- осуществлять загрузки файлов на компьютер ОУ без разрешения уполномоченного лица;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц, информацию, угрозы.

4. Уполномоченное лицо проверяет, является ли данный учащийся допущенным до самостоятельной работы в сети Интернет.

5. При случайном обнаружении лицом, работающим в сети Интернет, ресурса, содержимое которого несовместимо с целями образовательного процесса, он обязан незамедлительно покинуть данный ресурс и сообщить о таком ресурсе Уполномоченному лицу с указанием его доменного адреса.

Уполномоченное лицо обязано:

- принять сообщение лица, работающего в сети Интернет;
- довести информацию до сведения руководителя ОУ для оценки ресурса и принятия решения по политике доступа к нему в соответствии с п. 3 Политики настоящих Правил;
- направить информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения контентной фильтрации (в течение рабочего дня);
- если обнаруженный ресурс явно нарушает законодательство Российской Федерации – сообщить об обнаруженном ресурсе по специальной «горячей линии» для принятия уполномоченными организациями мер в соответствии с законодательством Российской Федерации (в течение суток).

Передаваемая информация должна содержать:

- Доменный адрес ресурса;
- Тематику ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо несовместимости с задачами образовательного процесса;
- Дату и время обнаружения;
- Информацию об установленных в ОУ технических средствах контентной фильтрации.

Регламент работы с электронной почтой в образовательной организации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Муниципальное общеобразовательное учреждение «Средняя общеобразовательная школа №15» имеет свой адрес электронной почты: blagodarsosh15@mail.ru .

1.2. Электронная почта в образовательном учреждении (далее Учреждение) может использоваться только в административных и образовательных целях. Пользователи и владельцы электронных почтовых ящиков должны соблюдать правила и инструкции по работе с электронной почтой, этические нормы общения.

1.3. Перед отправлением сообщения или отчета отправителю необходимо проверить правописание и грамматику текста.

Пользователям данного сервиса запрещено:

-участвовать в рассылке посланий, не связанных с образовательной или административной деятельностью Учреждения;

-пересылать по произвольным адресам не затребованную потребителями информацию (спам);

-отправлять сообщения противозаконного или неэтичного содержания;

-использовать массовую рассылку электронной почты, за исключением необходимых случаев;

-электронное послание не должно использоваться для пересылки секретной и конфиденциальной информации, регламент обмена которыми утверждается иными нормативно-правовыми актами .

2. ПОРЯДОК ОБРАБОТКИ, ПЕРЕДАЧИ И ПРИЕМА ДОКУМЕНТОВ ПО ЭЛЕКТРОННОЙ ПОЧТЕ

2.1. По электронной почте образовательной организации производится получение и отправка информации законодательного, нормативно-правового, учебного, учебно-методического характера а также любой другой информации, совместимой с процессом образования.

2.2. Для обработки, передачи и приема информации по электронной почте в Учреждении приказом директора назначается ответственное лицо – оператор электронной почты. При создании электронного почтового ящика , сайта Учреждения ответственное лицо направляет в муниципальный орган управления образованием свои электронные реквизиты для формирования базы данных образовательных учреждений.

Администрация Учреждения должна обеспечить бесперебойное функционирование сервиса электронной почты и регулярное получение и отpravку информации в течение всего рабочего дня.

2.3. Ответственность за ненадлежащую подготовку информации к передаче по электронной почте несет автор информации, предполагаемой к отправке; ответственность за отправку адресату и получение электронной почты – несет оператор электронной почты.

2.4. Все передаваемые учебно-методические и справочно-информационные материалы должны передаваться с сопроводительным письмом. Для отправки электронного сообщения пользователь оформляет документ в соответствии с требованиями по делопроизводству, утвержденными в образовательном учреждении.

При получении электронного сообщения оператор:

-передает документ на рассмотрение администрации Учреждения или в случае именного сообщения - непосредственно адресату;

-в случае невозможности прочтения электронного сообщения уведомляет об этом отправителя;

-ведет журнал приема-передачи электронной почты.

При оформлении электронного сообщения обязательны к заполнению следующие поля:

адрес получателя;

тема электронного сообщения;

текст электронного сообщения (при необходимости, могут быть вложены файлы);

подпись отправителя с указанием наименования образовательного учреждения и его структурного подразделения, сотрудником которого является отправитель.

2.6. Отправка и получение электронных документов осуществляется с использованием программных продуктов, предназначенных для работы с электронной почтой в образовательном учреждении.

2.8. Электронные документы дублируются в виде копий на бумажных носителях с присвоением номера входящего или исходящего документа. Сроки их хранения регламентируются иными нормативными актами.

3. ОТВЕТСТВЕННОСТЬ

3.1 Изменение наименования официального адреса электронного почтового ящика (ЭПЯ) Учреждения согласовывает с специалистами муниципального органа управления образованием, ведущими электронный документооборот и отвечающими за информатизацию системы муниципального образования.

3.2. По факту изменения официального ЭПЯ Учреждение обязано уведомить информационным письмом орган управления образованием за 3 рабочих дня до смены ЭПЯ с указанием даты, с которой изменения вступают в силу.

3.3 Ответственность за функционирование электронного документооборота в учреждении несет руководитель учреждения.

Инструкция по организации антивирусной защиты информационно-коммуникационной системы в образовательной организации

1. Общие положения

1.1.Целью создания системы антивирусной защиты 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 Учреждения к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

1.2.Основополагающими требованиями к системе антивирусной защиты Учреждения являются:

- решение задачи антивирусной защиты должно осуществляться в общем виде. Средство защиты не должно оказывать противодействие конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях) ничего не известно;
- решение задачи антивирусной защиты должно осуществляться в реальном времени.

1.3.Мероприятия, направленные на решение задач по антивирусной защите:

установка только лицензированного программного обеспечения либо бесплатное антивирусное программное обеспечение, идущее в комплекте с подлинной операционной системой (типа Microsoft Security Essentials (сеть до 10 рабочих станций) или Microsoft Forefront Endpoint Protection (сеть более 10 рабочих станций)), поддерживающее работу с пользовательскими профилями.

- регулярное обновление и ежедневные профилактические проверки (желательно в нерабочее ночное время);
- непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИКС;
- ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в ИКС операционного программного обеспечения и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика программного обеспечения и других специализированных экспертных антивирусных служб.
- проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными

службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.

- проведение регулярных проверок целостности критически важных программ и данных. Наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;

- внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования;

- необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;

- следует иметь планы обеспечения бесперебойной работы Учреждения для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

2. Технологические инструкции

2.1. В учреждении руководителем назначатся лицо, ответственное за антивирусную защиту, в должностные инструкции для которого должны быть прописаны порядок действия в период вирусных эпидемий, порядок действий при возникновении внештатных ситуаций, связанных с работоспособностью средств антивирусной защиты, порядок действий для устранения последствий заражений. В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя Учреждения.

2.2. В Учреждении может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (магнитных дисках, лентах, CD-ROM, DVD, flash-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

3. Требования к проведению мероприятий по антивирусной защите

3.1. В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.

3.2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю, данные, расположенные на рабочих станциях пользователей – ежедневно, в ночное время по расписанию.

3.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

3.3.1. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах учреждения.

3.3.2. 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 и т.п.).

3.3.3. При отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

3.4. В случае обнаружения зараженных вирусами файлов или электронных писем пользователи обязаны:

3.4.1. Приостановить работу.

3.4.2. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты (в случае его отсутствия – директора) Учреждения.

3.4.3. Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

3.4.4. Провести лечение или уничтожение зараженных файлов.

4. Ответственность

4.1. Ответственность за организацию антивирусной защиты возлагается на руководителя Учреждения или лицо, им назначенное.

4.2. Ответственность за проведение мероприятий антивирусного контроля в Учреждении возлагается на ответственного за обеспечение антивирусной защиты, соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

4.3. Периодический контроль за состоянием антивирусной защиты в Учреждении осуществляется руководителем и фиксируется Актом проверки (не реже 1 раз в квартал).