Муниципальное общеобразовательное учреждение

«Мининская основная общеобразовательная школа »

Тепло-Огаревского района Тульской области

ПРИКАЗ

30.09. 2009 № 71

О мерах по исключению доступа обучающихся к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания

Для решения задачи исключения доступа обучающихся МОУ «Мининская ООШ» Тепло-Огаревского района Тульской области к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания

ПИКАЗЫВАЮ:

1.Возложить ответственность за реализацию мер, обеспечивающих исключение доступа обучающихся МОУ «Мининская ООШ» к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, на учителя английского языка, ответственную за работу сети Интернет, Карпушкину Ю.В.

2.Утвердить:

2.1. Правила использования сети Интернет в МОУ «Мининская ООШ» (Приложение №1);

2.2. Инструкцию для сотрудников ОУ по вопросам регламентации доступа к информации в сети Интернет (Приложение № 2);

2.4. Должностную инструкцию ответственного за рабету точки доступа к сети Интернет в ОУ Приложение № 3;

2.5. Регламент работы сотрудников МОУ «Мининская ООШ» с электронной почтой (Приложение № 4);

2.6. Правила эксплуатации персонального компьютера (Приложение № 5).

3.Заместителю директора по УВР обеспечить:

3.1. контроль за исключением доступа обучающихся МОУ «Мининская ООШ» к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания;

3.2. деятельность МОУ «Мининская ООШ» по исключению доступа обучающихся к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, руководствуясь Классификатором информации, распространение которой запрещено в соответствии с законодательством Российской Федерации .

4. Контроль за исполнением приказа оставляю за собой.

Директор школы: Н.М.Сополькова

ПРИЛОЖЕНИЕ № 4
Утверждено
Приказ № 71 от 30.09.2009

Регламент работы сотрудников МОУ « Мининская ООШ» с электронной почтой

1. **Общие положения**

1.1. Электронная почта в муниципальном бюджетном общеобразовательном учреждении (далее — учреждение) может использоваться только в функциональных и образовательных целях.

1.2. Пользователи должны соблюдать правила и инструкции по работе с электронной почтой, этические нормы общения.

1.3. Перед отправлением сообщения необходимо проверять правописание и грамматику текста.

1.4. Пользователям запрещено:

1.4.1. Участвовать в рассылке посланий, не связанных с образовательным процессом.

1.4.2. Пересылать по произвольным адресам' не затребованную потребителями информацию (спам).

1.4.3. Отправлять сообщения противозаконного или неэтичного содержания.

1.4.4. Использовать массовую рассылку электронной почты, за исключением необходимых случаев.

1.5. Электронное послание не должно использоваться для пересылки секретной и конфиденциальной информации, поскольку является эквивалентом почтовой открытки.

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.

2.2. Для обработки, передачи и приема информации по электронной почте в учреждение приказом директора назначается ответственное лицо (секретарь ОУ)

2.3. При создании электронного ящика, сайта учреждения ответственное лицо направляет в управление образования свои электронные реквизиты для формирования базы данных.

2.4. Учреждение должно обеспечить бесперебойное функционирование электронной почты и получение информации не реже двух раз в день.

2.5. Ответственность за ненадлежащую подготовку информации к передаче по электронной почте несет ответственный за электронную почту.

2.6. Передаваемые с помощью электронной почты официальные документы должны иметь исходящий регистрационный номер.

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

2.8. При обучении работе с электронной почтой обучающихся ответственность за работу с почтой несет учитель.

2.9. Для отправки электронного сообщения пользователь оформляет документ в соответствии с требованиями, предъявляемыми к оформлению официальных документов, в электронном виде и представляет по локальной сети или на носителе информации ответственному лицу за электронную почту.

2.10. При получении электронного сообщения ответственное лицо за электронную почту:

2.10.1. Регистрирует документ в папке входящих документов;

2.10.2. Передает документ на рассмотрение директору или в случае указания непосредственно адресату.

2.10.3. В случае невозможности прочтения электронного сообщения уведомляет об этом отправителя.

ПРИЛОЖЕНИЕ № 1
Утверждено
Приказ № 71 от 30.09.2009

Правила использования сети Интернет

1. Общие положения

1.1 Настоящие Правила регулируют условия и порядок использования сети Интернет через ресурсы МОУ «Мининская ООШ» (далее - учреждение) учащимися, преподавателями и сотрудниками Школы.

1.2. Использование сети Интернет в учреждении направлено на решение задач учебно-воспитательного процесса.

1.3. Доступ к сети Интернет должен осуществляться только с использованием лицензионного или свободного программного обеспечения.

1.4 Настоящие Правила имеют статус локального нормативного акта учреждения.

2. Организация использования сети Интернет в МОУ « Миниская ООШ»

2.1 Вопросы использования возможностей сети Интернет в учебно- воспитательном процессе рассматриваются на педагогическом совете школы. Педагогический совет утверждает Правила использования сети Интернет на учебный год. Правила вводятся в действие приказом руководителя учреждения.

2.2 Правила использования сети Интернет разрабатываются педагогическим советом учреждения на основе данного регламента самостоятельно либо с привлечением внешних экспертов, в качестве которых могут выступать преподаватели других общеобразовательных учреждений, имеющие опыт использования Интернета в образовательном процессе, специалисты в области информационных технологий, представители управления образования, родители обучающихся.

2.3 При разработке правил использования сети Интернет педагогический совет руководствуется:
- законодательством Российской Федерации:
- уставом учреждения, образовательной программой;
- целями образовательного процесса;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов сети:
- интересами обучающихся.

2.4 Руководитель учреждения отвечает за эффективный и безопасный доступ к сети Интернет пользователей (сотрудников и учащихся школы), назначает в соответствии с

установленными правилами лицо, ответственное за организацию работы и ограничение доступа к сети Интернет, деятельность которого связана с образовательным процессом.

2.5 Педагогический совет учреждения принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет.

2.6 Во время уроков и других занятий в рамках учебного процесса контроль использования обучающимися сети Интернет осуществляет педагог, ведущий занятие. При этом педагог:

2.6.1 Наблюдает за использованием компьютеров в сети Интернет обучающимися.

Принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

2.7 Во время свободного доступа обучающихся к сети Интернет вне учебных занятий контроль использования ресурсов Интернета осуществляют работники учреждения, определенные приказом его руководителя.

Работник образовательного учреждения:

2.7.1. Наблюдает за использованием компьютера в сети Интернет обучающимися.

2.7.2. Принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

2.7.3. Сообщает классному руководителю о случаях нарушения обучающимися установленных Правил пользования Интернетом.

2.8 Контролирует объем трафика образовательного учреждения в сети Интернет.

2.9 При использовании сети Интернет в учреждении учащимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношение к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в учреждении или предоставленного оператором услуг связи.

2.10 Пользователи сети Интернет в учреждении должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим существует вероятность обнаружения обучающимися ресурсов. не имеющих отношения к образовательному процессу и содержание которых противоречит законодательству Российской Федерации. Общеобразовательное учреждение не несет ответственности за случайный доступ обучающихся к подобной информации, размещенной не на интернет-ресурсах учреждения.

2.11 При обнаружении указанной информации пользователю необходимо сообщить об этом ответственному за использование сети Интернет в учреждении, указав при этом адрес ресурса.

2.12 Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы. доступ к которым регулируется техническими средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в учреждении правилами обеспечивается руководителем или назначенным им работником.

2.13 Персональные данные педагогических работников и обучающихся (включая фамилию и имя. класс/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр.. иные сведения личного характера) могут размещаться на интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.

2.14 При получении согласия на размещение персональных данных представитель учреждения обязан разъяснить возможные риски и последствия их опубликования. Учреждение не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

3. Права, обязанности и ответственность пользователей

3.1 Использование сети Интернет в учреждении осуществляется в целях образовательного процесса.

3.2 Преподаватели, сотрудники и обучающиеся могут бесплатно пользоваться доступом к глобальным интернет-ресурсам по разрешению лица, назначенного ответственным за организацию в учреждении работы сети Интернет и ограничению доступа.

3.3 К работе в сети Интернет допускаются лица, прошедшие инструктаж и обязавшиеся соблюдать правила работы.

3.4 Перед работой пользователю необходимо расписаться в журнале учета работы в сети Интернет.

3.5 За одним рабочим столом должно находиться не более одного пользователя.

ПРИЛОЖЕНИЕ № 5
Утверждено
Приказ № 71 от 30.09.2009

Правила эксплуатации персонального компьютера

1. Необходимо обеспечить защиту ПК от воздействия пыли. Не желательно устанавливаться системный блок на пол, потому что именно так пыль быстрее всего проникает внутрь. Но, не смотря на все меры защиты, пыль, так или иначе, попадает в системный блок, и необходимо своевременно проводить техническое обслуживание ПК. Для чего оно проводится? Из-за воздействия пыли, происходит перегрев компонентов системного блока, помимо этого забиваются контакты, что приводит к выходу из строя того или иного устройства. Чистку системного блока необходимо проводить 2-3 раза в год. Не рекомендуется делать это самостоятельно, так как данная процедура имеет множество нюансов и сложностей.
2. Необходимо поддерживать температурный баланс в системном блоке, так как при высоких температурах компоненты ПК очень быстро изнашиваются, либо не корректно работают. Температура каждого комплектующего должна быть в пределах нормы, все кулера (вентиляторы) должны быть в хорошем рабочем состоянии
3. ПК не должен располагаться под прямыми солнечными лучами, желательно обеспечить возможность для хорошей циркуляции воздуха.
4. Не рекомендуется самостоятельно вскрывать системный блок и производить какие-либо действия с его содержимым, потому что достаточно малейшего прикосновения, для того что бы вывести из строя ту или иную запчасть.
5. На вашем ПК обязательно должен быть установлена антивирусная программа, а так же программа для защиты от вирусов, проникающих с флеш-карт. Перед использованием, любой внешний носитель информации (флеш-карта/диск), а так же информацию, скачанную с интернета необходимо просканировать антивирусной программой. Необходимо проследить, что бы при подключении к Internet ежедневно обновлялись антивирусные базы, если подключение отсутствует, делать это вручную.
6. Рекомендуется не посещать сомнительные сайты, не устанавливать пиратские программы. Так же не рекомендуется “перегружать” операционную систему большим количеством не используемых программ, свои документы, личные файлы держать в порядке, не используемую информацию удалять.
7. Все шнуры, используемые для соединения ПК с другими устройствами вставлять и вынимать можно только при выключенном компьютере, иначе можно сжечь порт, куда вставляется кабель. Исключение:USB-порты.
8. Необходимо ВСЕГДА производить правильное отключение компьютера (Пуск—»Завершение работы—»Выключение)
9. Рекомендуется использовать источник бесперебойного питания (ИБП). В случае отключения электропитания, ИБП обеспечит подачу питания для работы ПК, что позволяет сохранить необходимую информацию и произвести корректное отключение. Так же он стабилизирует напряжение, что не мало важно, потому что скачки напряжений/молнии, наносят большой ущерб любой техники, а особенно компьютеру, вплоть до выхода из строя.

ПРИЛОЖЕНИЕ № 2
Утверждено
Приказ № 71 от 30.09.2009

Инструкция
для работников образовательного учреждения по вопросам регламентации доступа к информации в сети Интернет

1. Общие сведения

1.1. Использование сети Интернет в ОУ 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. Точка доступа к Интернету – оборудованное помещение для организации доступа к ресурсам сети Интернет в ОУ.

1.3. Пользователи точки доступа к Интернету могут бесплатно пользоваться доступом к глобальным Интернет-ресурсам, искать необходимую информацию, размещать собственную. Также они могут получать консультации по вопросам, связанным с использованием сети Интернет.

2. Организация использования сети Интернет

2.1. Пользователями точки доступа являются работники ОУ и обучающиеся.

2.2. Использование сети Интернет в ОУ возможно исключительно при условии ознакомления и согласия лица, пользующегося сетью Интернет в ОУ, с Правилами использования сети Интернет в общеобразовательном учреждении (далее – Правила), которое удостоверяется подписью лица в Листе ознакомления с Правилами.

2.3. Во время занятий контроль за использованием обучающимися ресурсов сети Интернет в соответствии с Правилами осуществляет преподаватель.

Преподаватель:
– наблюдает за использованием компьютера и сети Интернет обучающимися;
– запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения им Правил и иных нормативных документов, регламентирующих использование сети Интернет в ОУ;
– принимает предусмотренные Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу / группе ресурсов, несовместимых с задачами образования.

2.4. Использование сети Интернет во внеучебное время может осуществляться только уполномоченным лицом (учителем информатики) либо под его постоянным контролем.

Уполномоченное лицо:
– проверяет, является ли данный обучающийся допущенным до самостоятельной работы в сети Интернет;

– определяет время и место для свободной работы в сети Интернет пользователей с учётом использования соответствующих технических мощностей ОУ в образовательном процессе, а также длительность сеанса работы одного человека;

– контролирует использование компьютера и сети Интернет обучающимися;

– запрещает дальнейшую работу пользователя в сети Интернет в случае нарушения пользователем Правил и иных нормативных документов, регламентирующих использование сети Интернет в образовательном учреждении;

– принимает предусмотренные Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу / группе ресурсов, не совместимых с задачами образования.

3. Интернет-ресурсы необразовательной направленности

3.1. Пользователю запрещается:

– посещать ресурсы, содержащие информацию, противоречащую законодательству РФ или не совместимую с целями воспитания и образования;

– осуществлять любые сделки через Интернет, распространять рекламную, коммерческую или схожую по направленности информацию;

– участвовать в чатах, конференциях, форумах необразовательной направленности;

– пользоваться аккаунтами (в том числе и собственными) социальных сетей,

– распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.2. При случайном обнаружении лицом, работающим в сети Интернет, ресурса, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно покинуть данный ресурс и сообщить о нём уполномоченному лицу.

4. Технические ограничения на использование точки доступа к Интернету

4.1. Пользователям запрещается:

– осуществлять загрузки файлов на компьютер ОУ без разрешения уполномоченного лица;

– устанавливать на компьютерах дополнительное программное обеспечение, как полученное в Интернете, так и любое другое;

– изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нём (заставки, картинку рабочего стола, стартовой страницы браузера), если это не определено преподавателем как учебное задание;

– включать, выключать и перезагружать компьютер без согласования с ответственным за точку доступа к Интернету.

Муниципальное общеобразовательное учреждение
«Мининская основная общеобразовательная школа»
Тепло-Огаревского района Тульской области

ПРИКАЗ

30.12.2009 № 82

Об утверждении Положения о совете ОУ по вопросам регламентации доступа к информации в сети Интернет

Для реализации комплексных мер по внедрению и использованию программно-технических средств контентной фильтрации, доступа обучающихся МОУ «Мининская ООШ» к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами обучения и воспитания

ПРИКАЗЫВАЮ:

1. Утвердить Положение о совете МОУ «Мининская ООШ» по вопросам регламентации доступа к информации в сети Интернет .
2. Контроль за выполнением настоящего приказа возложить на зам. директора по УВР Попову О.В

Директор школы: Н.М.Сополькова

Принято:	Утверждаю:
на заседании педагогического совета Протокол № 4 от 30.12.2009	Директор школы: Н.М.Сополькова Приказ № 82 от 30.12.2009

Положение

о совете ОУ по вопросам регламентации доступа к информации в сети Интернет

1**. Общие положения.**

1.1. В соответствии с настоящим Положением о совете образовательного учреждения по вопросам регламентации доступа к информации в Интернете (далее - Совет) целью создания Совета является принятие мер по ограничению доступа обучающихся к ресурсам сети Интернет, содержащим информацию, не имеющую отношения к образовательному процессу.

1.2. Совет осуществляет непосредственное определение политики доступа в Интернет.

1.3. Совет создается из представителей педагогического коллектива, родительского комитета (попечительского совета) и ученического самоуправления в согласованном порядке.

1.4. Очередные собрания Совета проводятся с периодичностью, установленной Советом.

2. **Компетенции Совета:**

2.1. Принимает решения на основе методических рекомендаций и классификационных списков ресурсов о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет, содержащим информацию, не имеющую отношения к образовательному процессу, с учетом социокультурных особенностей конкретного региона, мнения членов Совета, а также иных заинтересованных лиц, представивших свои предложения в Совет;

2.2. Определяет характер и объем информации, публикуемой на интернет-ресурсах образовательного учреждения;

2.3. Направляет руководителю образовательного учреждения рекомендации о назначении и освобождении от исполнения своих функций сотрудников, ответственных за непосредственный контроль безопасности работы обучающихся в сети Интернет и ее соответствия целям и задачам образовательного процесса.

3. **Организация работы Совета**.

3.1. Принятие решений о политике доступа к ресурсам/группам ресурсов сети Интернет осуществляется Советом самостоятельно с привлечением внешних экспертов:

- преподавателей образовательного учреждения и других образовательных учреждений;
- специалистов в области информационных технологий и обеспечения безопасного доступа;
- представителей органов управления образованием.

4. **Права и ответственность членов совета.**

4.1.. При принятии решений Совет должен руководствоваться:

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

4.2. Отнесение определенных категорий и/или ресурсов к соответствующим группам, доступ к которым регулируется техническими средствами и программным обеспечением ограничения доступа к информации, осуществляется на основании решений Совета лицом, уполномоченным руководителем образовательного учреждения по представлению Совета.

4.3. Категории ресурсов, в соответствии с которыми определяется политика использования сети Интернет в образовательном учреждении, доступ к которым регулируется техническими средствами и программным обеспечением технического ограничения доступа к информации, определяются в установленном порядке.

Муниципальное общеобразовательное учреждение

«Мининская основная общеобразовательная школа »

Тепло-Огаревского района Тульской области

ПРИКАЗ

30.12.2009 № 83

Об утверждении состава совета
ОУ по вопросам регламентации доступа
к информации в сети Интернет.

На основании положения о совете МОУ «Мининская ООШ» по вопросам регламентации доступа к информации в сети Интернет, решения педагогического совета № 4 от 30.12.2009г., для принятия мер для исключения доступа обучающихся к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания обучающихся
ПРИКАЗЫВАЮ:
Утвердить

1.Состав совета ОУ из числа представителей педагогического коллектива, профсоюзной организации и ученического самоуправления:

- Попова Оксана Викторовна, заместитель директора по УВР;
- Карпушкина Юлия Валерьевна, учитель английского языка;
- Солкуцан Оксана Владимировна, председатель ПК;
- Еремина Яна Юрьевна, учащаяся 8 класса;
- Миронов Олег Юрьевич, учащийся 9 класса.

2.Инструкцию о порядке действий при осуществлении контроля за использованием обучающимися сети Интернет (Приложение № 1).

3. Порядок разработки системы классификации информации, несовместимой с задачами образования и воспитания обучающихся, и применения указанной системы классификации (Приложение № 2)

4. Классификатор информации, несовместимой с задачами образования и воспитания обучающихся (Приложение № 3)

Директор школы: Н.М.Сопольков

ПРИЛОЖЕНИЕ 1
УТВЕРЖДЕНО

Приказом директора школы
от 30.12.2009 № 83

ИНСТРУКЦИЯ
о порядке действий при осуществлении контроля за использованием обучающимися сети Интернет МОУ «Мининская ООШ»

1. Настоящая Инструкция устанавливает для сотрудников и членов совета образовательного учреждения по вопросам регламентации доступа к информации в Интернете МОУ «Мининская ООШ» порядок действий при обнаружении:

1) возможности доступа обучающихся к потенциально опасному контенту;
2) вызванного техническими причинами отказа доступа к контенту, не представляющему опасности для обучающихся, доступ к которому не противоречит принятым нормативным актам на федеральном уровне, уровне Волгоградской области, как субъекта Российской Федерации, муниципальном уровне, а также на уровне образовательного учреждения.
2. Контроль за использованием обучающимися сети Интернет осуществляют:
1) во время проведения занятий – преподаватель, проводящий занятие и/или лицо, специально уполномоченное руководством образовательного учреждения на осуществление такого контроля;
2) во время использования сети Интернет для свободной работы обучающихся - лицо, уполномоченное советом образовательного учреждения по вопросам регламентации доступа к информации в Интернете (далее – "Совет") или руководителем образовательного учреждения в установленном Советом порядке.
3. Лицо, осуществляющее контроль за использованием обучающимися сети Интернет:
- определяет время и место работы обучающихся в сети Интернет с учетом использования соответствующих технических возможностей в образовательном процессе, а также длительность сеанса работы одного обучающегося;
- способствует осуществлению контроля за объемом трафика образовательного учреждения в сети Интернет;
- наблюдает за использованием компьютеров и сети Интернет обучающимися;
- запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения обучающимся порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;
- не допускает обучающегося к работе в сети Интернет в предусмотренных Правилами использования сети Интернет случаях;

принимает необходимые меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования и воспитания обучающихся.

4. При обнаружении информации, в отношении которой у лица, осуществляющего контроль за использованием обучающимися сети Интернет, возникают основания предполагать, что такая информация относится к числу запрещенной для распространения в соответствии с законодательством Российской Федерации или иному потенциально опасному для обучающихся контенту, ответственное лицо направляет соответствующую информацию руководителю образовательного учреждения и в Совет, которые принимают необходимые решения.

5. При обнаружении вызванного техническими причинами отказа доступа к контенту, не представляющему опасности для обучающихся, доступ к которому не противоречит принятым нормативным актам на федеральном уровне, уровне Тульской области, как субъекта Российской Федерации, муниципальном уровне, а также на уровне образовательного учреждения, ответственное лицо направляет соответствующую информацию по специальной "горячей линии" для принятия соответствующих мер по восстановлению доступа к разрешенному контенту.

Директор школы: Н.М.Сополькова

ПРИЛОЖЕНИЕ 2
УТВЕРЖДЕНО

Приказом директора школы
от 30.12.2009 № 83

Порядок разработки системы классификации информации, несовместимой с задачами образования и воспитания обучающихся, и применения указанной системы классификации

1. Настоящий Порядок содержит рекомендации, касающиеся порядка разработки системы классификации информации, несовместимой с задачами образования и воспитания обучающихся, и применения указанной системы классификации в целях исключения доступа обучающихся МОУ «Мининская ООШ» к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания обучающихся.

2. Классификацию информации, запрещенной законодательством Российской Федерации к распространению и несовместимой с задачами образования и воспитания обучающихся, осуществляет Совет.
3. Классификатор информации, запрещенной законодательством Российской Федерации к распространению, применяется в единообразном виде на всей территории Российской Федерации.
4. Классификатор информации, несовместимой с задачами образования и воспитания обучающихся, может содержать части (разделы), рекомендуемые к применению в единообразном виде на всей территории Российской Федерации и части (разделы), рекомендации по применению которых даются экспертно-консультативными органами (советами) регионального и (или) муниципального уровня.
5. Общественный совет является независимыми органами.
6. В соответствии с законодательством Российской Федерации образовательное учреждение свободно в выборе и применении классификаторов информации, несовместимой с задачами образования и воспитания обучающихся, а также несет ответственность за невыполнение функций, отнесенных к его компетенции.
7.Классификатор информации, несовместимой с задачами образования и воспитания обучающихся, разрабатывается и Общественным советом и утверждается директором школы.

Директор школы: Н.М.Сополькова

ПРИЛОЖЕНИЕ 3
УТВЕРЖДЕНО
Приказом директора школы
от 30.12.2009 № 83

Классификатор
информации, несовместимой с задачами образования и воспитания обучающихся

№ п / п	Наименование тематической категории	Содержание
1	2	3
1.	Алкоголь	Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию.
2.	Баннеры и рекламные программы	Баннерные сети, всплывающая реклама, рекламные программы.
3.	Вождение и автомобили (ресурсы данной категории, несовместимые с задачами образования)	Несовместимая с задачами образования и воспитания информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям.
4.	Досуг и развлечения (ресурсы данной категории, несовместимые с задачами образования)	Несовместимая с задачами образования и воспитания информация в виде фотоальбомов и рейтингов фотографий, открыток, гороскопов, сонников, гаданий, магии, астрологии, ТВ-программ, прогнозов погоды, тестов, рейтингов, фотоконкурсов, конкурсов онлайн, несовместимая с задачами образования и воспитания информация о туризме, путешествиях, тостах, поздравлениях, кроссвордах, сканвордах, ответов к ним, фэнтези и фантастике, кулинарии, рецептах, диетах, моде, одежде, обуви, модных аксессуарах, показах мод, текстах песен, кино, киноактерах, расписаниях концертов, спектаклей, кинофильмов, заказе билетов в театры, кино и т.п., дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними, рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании, службах знакомств, размещении объявлений онлайн, анекдотах, приколах, слухах, сайтах и журналы для женщин и для мужчин, желтая пресса, онлайн-ТВ, онлайн радио, знаменитости, косметика, парфюмерия, прически, ювелирные украшения.
5.	Здоровье и медицина (ресурсы данной категории, несовместимые с задачами образования)	Несовместимая с задачами образования и воспитания информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иных материалах по теме "Здоровье и медицина", которые, являясь академическими, по сути, могут быть также отнесены к другим категориям, например, порнография, трупы и т.п.
6.	Компьютерные игры (ресурсы данной категории, несовместимые с задачами образования)	Несовместимая с задачами образования и воспитания компьютерные онлайновые и оффлайновые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты.
7.	Корпоративные сайты, Интернет - представительства негосударственных учреждений (ресурсы данной категории, несовместимые с задачами образования)	Содержащие несовместимую с задачами образования и воспитания информацию сайты коммерческих фирм, компаний, предприятий, организаций.
8.	Личная и немодерируемая информация	Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию

№ п / п	Наименование тематической категории	Содержание
1	2	3
		(адреса, телефоны и т. п.), личные странички, дневники, блоги.
9.	Отправка SMS с использованием Интернет-ресурсов	Сайты, предлагающие услуги по отправке SMS-сообщений
10.	Модерируемые доски объявлений (ресурсы данной категории, несовместимые с задачами образования)	Содержащие несовместимую с задачами образования и воспитания информацию модерируемые доски сообщений/объявлений, а также модерируемые чаты.
11.	Нелегальная помощь школьникам и студентам	Банки готовых рефератов, эссе, дипломных работ и проч.
12.	Неприличный и грубый юмор	Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека.
13.	Нижнее белье, купальники	Сайты, на которых рекламируется и изображается нижнее белье и купальники.
14.	Обеспечение анонимности пользователя, обход контентных фильтров	Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам. Peer-to-Peer программы, сервисы бесплатных прокси - серверов, сервисы, дающие пользователю анонимность
15.	Онлайн - казино и тотализаторы	Электронные казино, тотализаторы, игры на деньги, конкурсы и проч.
16.	Платные сайты	Сайты, на которых вывешено объявление о платности посещения веб-страниц.
17.	Поиск работы, резюме, вакансии (ресурсы данной категории, несовместимые с задачами образования)	Содержащие несовместимую с задачами образования и воспитания Интернет-представительства кадровых агентств, банки вакансий и резюме.
18.	Поисковые системы (ресурсы данной категории, несовместимые с задачами образования)	Содержащие несовместимую с задачами образования и воспитания Интернет-каталоги, системы поиска и навигации в Интернете.
19.	Религии и атеизм (ресурсы данной категории, несовместимые с задачами образования)	Сайты, содержащие несовместимую с задачами образования и воспитания информацию религиозной и антирелигиозной направленности
20.	Системы поиска изображений	Системы для поиска изображений в Интернете по ключевому слову или словосочетанию.
21.	СМИ (ресурсы данной категории, несовместимые с задачами образования)	Содержащие несовместимую с задачами образования и воспитания информацию новостные ресурсы и сайты СМИ (радио, телевидения, печати)
22.	Табак, реклама табака, пропаганда потребления табака	Сайты, пропагандирующие потребление табака. Реклама табака и изделий из него.
23.	Торговля и реклама (ресурсы данной	Содержащие несовместимую с задачами образования и воспитания информацию сайты следующих категорий: аукционы, распродажи

№ п / п	Наименование тематической категории	Содержание
1	2	3
	категории, несовместимые с задачами образования)	онлайн, Интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, недвижимость, аренда недвижимости, покупка недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в Интернете, е-бизнес
24.	Убийства, насилие	Сайты, содержащие описания или изображения убийств, мертвых тел, насилия и т. п.
25.	Чаты (ресурсы данной категории, несовместимые с задачами образования)	Несовместимые с задачами образования и воспитания сайты для анонимного общения в режиме онлайн.

Директор школы: Н.М.Сополькова

Муниципальное казенное общеобразовательное учреждение
«Мининская основная общеобразовательная школа»

П Р И К А З

18.10.2012 № 69

Об утверждении правил, инструкций, регламента работы по запуску и обновлению антивирусного программного обеспечения

В рамках реализации приоритетного национального проекта «Образование» с целью обеспечения доступа учителей и учащихся к сети Интернет,

ПРИКАЗЫВАЮ:
утвердить:

1. регламент по запуску и обновлению антивирусного программного обеспечения (приложение №1).
2. инструкцию по организации антивирусной защиты компьютерной техники (приложение № 2)

Директор школы: Н.М.Сополькова

Муниципальное казенное общеобразовательное учреждение
«Мининская основная общеобразовательная школа»

П Р И К А З

28.10.2012 № 70

О назначении лица, ответственного за работу Интернет и внедрение системы контент -фильтрации в ОУ и утверждении положений и инструкций.

Для организации системной работы сети Интернет в МКОУ «Мининская ООШ» и внедрения контент -фильтрации в ОУ

ПРИКАЗЫВАЮ:

1. Назначить ответственной за работу сети Интернет в МКОУ «Мининская ООШ» учителя начальных классов Прусакову Надежду Сергеевну
2. Утвердить должностную инструкцию ответственного за работу сети Интернет и внедрение системы контент – фильтрации в ОУ (Приложение № 1).
3. Утвердить Положение об информационном узле (сайте) ОУ, принятое на заседании педагогического совета (протокол № 2 от 28.10.2012. Приложение № 2).
4. Утвердить положение о порядке обработки и обеспечении безопасности персональных данных в ОУ, принятое на заседании педагогического совета (протокол № 2 от 28.10.2012. Приложение № 3).

Директор школы: Н.М.Сополькова

ПРИЛОЖЕНИЕ 2
УТВЕРЖДЕНО
Приказом директора школы
от 18.10.2012 № 69

Инструкция по организации антивирусной защиты компьютерной техники

1.Общие положения

1.1 В муниципальном общеобразовательном учреждении «Мининская основная общеобразовательная школа» (далее - учреждение) руководителем должно быть назначено лицо, ответственное за антивирусную защиту.

1.2 В учреждении может использоваться только лицензионное антивирусное программное обеспечение.

1.3 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

2. Требования к проведению мероприятий по антивирусной защите

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

2.2 Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.

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

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

2.5 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.).

2.6 При отправке и получении электронной почты пользователь обязан проверить электронные письма на наличие вирусов.

2.7 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

- Приостановить работу.
- Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в учреждении.
- Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.
- Провести лечение или уничтожение зараженных файлов.

3. Ответственность

3.1 Ответственность за организацию антивирусной защиты возлагается на руководителя учреждения или лицо, им назначенное.

3.2 Ответственность за проведение мероприятий антивирусного контроля в учреждении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение антивирусной защиты.

3.3 Периодический контроль за состоянием антивирусной защиты в учреждении осуществляется руководителем.

Директор школы: Н.М.Сопольков

ПРИЛОЖЕНИЕ 2
УТВЕРЖДЕНО
Приказом директора школы
от 18.10.2012 № 69

РЕГЛАМЕНТЫ РАБОТЫ

по запуску и обновлению антивирусного программного обеспечения

В качестве источника угроз информационной безопасности может выступать человек либо группа людей, а также некие, независящие от деятельности человека, проявления. Исходя из этого, все источники угроз можно разделить на три группы:

- **Человеческий фактор**. Данная группа угроз связана с действиями человека, имеющего санкционированный или несанкционированный доступ к информации. Угрозы этой группы можно разделить на:
- внешние, к ним относятся действия кибер-преступников, хакеров, интернет-мошенников, недобросовестных партнеров, криминальных структур.
- внутренние, к ним относятся действия персонала компаний, а также пользователей домашних компьютеров. Действия данных людей могут быть как умышленными, так и случайными.
- **Технический фактор**. Эта группа угроз связана с техническими проблемами – физическое и моральное устаревание использующегося оборудования, некачественные программные и аппаратные средства обработки информации. Все это приводит к отказу оборудования и зачастую потери информации.
- **Стихийный фактор**. Эта группа угроз включает в себя природные катаклизмы, стихийные бедствия и прочие форс-мажорные обстоятельства, независящие от деятельности людей.

Все три источника угроз необходимо обязательно учитывать при разработке системы защиты информационной безопасности.

Развитие современных компьютерных технологий и средств связи дает возможность злоумышленникам использовать различные источники распространения угроз. Рассмотрим их подробнее:

Интернет

Глобальная сеть Интернет уникальна тем, что не является чьей-то собственностью и не имеет территориальных границ. Это во многом способствует развитию многочисленных веб-ресурсов и обмену информацией. Сейчас любой человек может получить доступ к данным, хранящимся в Интернете, или создать свой собственный веб-ресурс.

Однако эти же особенности глобальной сети предоставляют злоумышленникам возможность совершения преступлений в Интернете, при этом затрудняя их обнаружение и наказание.

Злоумышленники размещают вирусы и другие вредоносные программы на веб-ресурсах, "маскируют" их под полезное и бесплатное программное обеспечение. Кроме того, скрипты, автоматически запускаемые при открытии веб-страницы, могут выполнять вредоносные действия на вашем компьютере, включая изменение системного реестра, кражу личных данных и установку вредоносного программного обеспечения.

Используя сетевые технологии, злоумышленники реализуют атаки на удаленные частные компьютеры и сервера компаний. Результатом таких атак может являться выведение ресурса из строя, получение полного доступа к ресурсу, а, следовательно, к информации, хранящемся на нем, использование ресурса как части зомби-сети.

В связи с появлением кредитных карт, электронных денег и возможностью их использования через Интернет (интернет-магазины, аукционы, персональные страницы банков и т.д.) интернет-мошенничество стало одним из наиболее распространенных преступлений.

Интранет

Интранет – это внутренняя сеть, специально разработанная для управления информацией внутри компании или, например, частной домашней сети. Интранет является единым пространством для хранения, обмена и доступа к информации для всех компьютеров сети. Поэтому, если какой-либо из компьютеров сети заражен, остальные компьютеры подвергаются огромному риску заражения. Во избежание возникновения таких ситуаций необходимо защищать не только периметр сети, но и каждый отдельный компьютер.

Электронная почта

Наличие почтовых приложений практически на каждом компьютере, а также то, что вредоносные программы полностью используют содержимое электронных адресных книг для выявления новых жертв, обеспечивает благоприятные условия для распространения вредоносных программ. Пользователь зараженного компьютера, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т.д. Нередки случаи, когда зараженный файл-документ по причине недосмотра попадает в списки рассылки коммерческой информации какой-либо крупной компании. В этом случае страдают не пять, а сотни или даже тысячи абонентов таких рассылок, которые затем разошлют зараженные файлы десяткам тысячам своих абонентов.

Помимо угрозы проникновения вредоносных программ существуют проблема внешней нежелательной почты рекламного характера (спама). Не являясь источником прямой угрозы, нежелательная корреспонденция увеличивает нагрузку на почтовые сервера, создает дополнительный трафик, засоряет почтовый ящик пользователя, ведет к потере рабочего времени и тем самым наносит значительный финансовый урон.

Также важно отметить, что злоумышленники стали использовать так называемые спамерские технологии массового распространения и методы социального инжиниринга, чтобы заставить пользователя открыть письмо, перейти по ссылке из письма на некий интернет-ресурс и т.п. Из этого следует, что возможности фильтрации спама важны не

только сами по себе, но и для противодействия некоторым новым видам интернет-мошенничества (например, фишингу), а также распространению вредоносных программ.

Съемные носители информации

Съемные носители – дискеты, CD-диски, флеш-карты – широко используются для хранения и передачи информации.

При запуске файла, содержащего вредоносный код, со съемного носителя вы можете повредить данные, хранящиеся на вашем компьютере, а также распространить вирус на другие диски компьютера или компьютеры сети.

Виды угроз.

Черви (Worms)

Данная категория вредоносных программ для распространения использует в основном уязвимости операционных систем. Название этого класса было дано исходя из способности червей "переползать" с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Также благодаря этому многие черви обладают достаточно высокой скоростью распространения.

Черви проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Вирусы (Viruses)

Программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение.

Троянские программы (Trojans)

Программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к "зависанию", воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом "полезного" программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

В последнее время наиболее распространенными типами вредоносных программ, портящими компьютерные данные, стали черви. Далее по распространенности следуют вирусы и троянские программы. Некоторые вредоносные программы совмещают в себе характеристики двух или даже трех из перечисленных выше классов.

Программы-рекламы (Adware)

Программный код, без ведома пользователя включенный в программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе, изменяют различные параметры браузера (стартовые и поисковые страницы, уровни безопасности и т.д.), а также создают неконтролируемый пользователем трафик. Все это может привести как к нарушению политики безопасности, так и к прямым финансовым потерям.

Программы-шпионы (Spyware)

Программное обеспечение, позволяющее собирать сведения об отдельно взятом пользователе или организации без их ведома. О наличии программ-шпионов на своем компьютере вы можете и не догадываться. Как правило, целью программ-шпионов является:

- отслеживание действий пользователя на компьютере;
- сбор информации о содержании жесткого диска; в этом случает чаще всего речь идет о сканировании некоторых каталогов и системного реестра с целью составления списка программного обеспечения, установленного на компьютере;
- сбор информации о качестве связи, способе подключения, скорости модема и т.д.

Потенциально опасные приложения (Riskware)

Программное обеспечение, которое не имеет какой-либо вредоносной функции, но может быть использовано злоумышленниками в качестве вспомогательных компонентов вредоносной программы, поскольку содержит бреши и ошибки. При некоторых условиях наличие таких программ на компьютере подвергает ваши данные риску. К таким программам относятся, например, некоторые утилиты удаленного администрирования, программы автоматического переключения раскладки клавиатуры, IRC-клиенты, FTP-сервера, всевозможные утилиты для остановки процессов или скрытия их работы.

Еще одним видом вредоносных программ, являющимся пограничным для таких программ как Adware, Spyware и Riskware, являются программы, встраивающиеся в установленный на компьютере браузер и перенаправляющие трафик.

Программы-шутки (Jokes)

Программное обеспечение, не причиняющее компьютеру какого-либо прямого вреда, но выводящее сообщения о том, что такой вред уже причинен, либо будет причинен при

каких-либо условиях. Такие программы часто предупреждают пользователя о несуществующей опасности, например, выводят сообщения о форматировании диска (хотя никакого форматирования на самом деле не происходит), обнаруживают вирусы в незараженных файлах и т.д.

Программы-маскировщики (Rootkit)

Утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Программы-маскировщики модифицируют операционную систему на компьютере и заменять основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Прочие опасные программы

Программы, созданные для организации DoS-атак на удаленные сервера, взлома других компьютеров, а также являющиеся частью среды разработки вредоносного программного обеспечения. К таким программам относятся хакерские утилиты (Hack Tools), конструкторы вирусов, сканеры уязвимостей, программы для взлома паролей, прочие виды программ для взлома сетевых ресурсов или проникновения в атакуемую систему.

Хакерские атаки

Хакерские атаки – это действия злоумышленников или вредоносных программ, направленные на захват информационных данных удаленного компьютера, выведение системы из строя или получение полного контроля над ресурсами компьютера.

Некоторые виды интернет-мошенничества

Фишинг (Phishing) – вид интернет-мошенничества, заключающийся в рассылке электронных сообщений с целью кражи конфиденциальной информации, как правило, финансового характера. Фишинг-сообщения составляются таким образом, чтобы максимально походить на информационные письма от банковских структур, компаний известных брендов. Письма содержат ссылку на заведомо ложный сайт, специально подготовленный злоумышленниками и являющийся копией сайта организации, от якобы имени которой пришло письмо. На данном сайте пользователю предлагается ввести, например, номер своей кредитной карты и другую конфиденциальную информацию.

Дозвон на платные интернет-ресурсы – вид интернет-мошенничества, связанный с несанкционированным использованием платных интернет-ресурсов (чаще всего это веб-сайты порнографического содержания). Установленные злоумышленниками программы (dialers) инициируют модемное соединение с вашего компьютера на платный номер. Чаще

всего используемые номера имеют очень высокие тарифы, в результате пользователь вынужден оплачивать огромные телефонные счета.

Навязчивая реклама

Навязчивая реклама – это всплывающие окна и рекламные баннеры, открывающиеся при работе с веб-сайтами. Как правило, информация, содержащаяся в них, не бывает полезной. Демонстрация всплывающих окон и баннеров отвлекает пользователя от основных задач, увеличивает объем трафика.

Спам (Spam)

Спам – это анонимная массовая рассылка нежелательных почтовых сообщений. Так, спамом являются рассылки рекламного, политического и агитационного характера, письма, призывающие помочь кому-нибудь. Отдельную категорию спама составляют письма с предложениями обналичить большую сумму денег или вовлекающие в финансовые пирамиды, а также письма, направленные на кражу паролей и номеров кредитных карт, письма с просьбой переслать знакомым (например, письма счастья) и т. п. Спам существенно увеличивает нагрузку на почтовые сервера и повышает риск потери информации, важной для пользователя.

Признаки заражения

Есть ряд признаков, свидетельствующих о заражении компьютера. Если вы замечаете, что с компьютером происходят "странные" вещи, а именно:

- на экран выводятся непредусмотренные сообщения, изображения либо воспроизводятся непредусмотренные звуковые сигналы;
- неожиданно открывается и закрывается лоток CD/DVD-ROM-устройства;
- произвольно, без вашего участия, на вашем компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя вы никак не инициировали такое ее поведение,

то, с большой степенью вероятности, можно предположить, что ваш компьютер поражен вирусом.

Кроме того, есть некоторые характерные признаки поражения вирусом через почту:

- друзья или знакомые говорят вам о сообщениях от вас, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Следует отметить, что не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. Например, в случае с почтой зараженные сообщения могут рассылаться с вашим обратным адресом, но не с вашего компьютера.

Есть также косвенные признаки заражения вашего компьютера:

 частые зависания и сбои в работе компьютера;
 медленная работа компьютера при запуске программ;
 невозможность загрузки операционной системы;
 исчезновение файлов и каталогов или искажение их содержимого;
 частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
 веб-браузер (например, Microsoft Internet Explorer) "зависает" или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении.

Что делать при наличии признаков заражения

Если вы заметили, что ваш компьютер "ведет себя подозрительно",

 Отключите компьютер от интернета и локальной сети, если он к ней был подключен.
 Если симптом заражения состоит в том, что вы не можете загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Microsoft Windows, который вы создавали при установке операционной системы на компьютер.
 Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы на внешний носитель (дискету, CD-диск, флеш-карту и пр.).
 Установите антивирусную программу, если вы этого еще не сделали.
 Обновите сигнатуру угроз программы. Если это возможно, для их получения выходите в интернет не со своего компьютера, а с незараженного компьютера друзей, интернет-кафе, с работы. Лучше воспользоваться другим компьютером, поскольку при подключении к интернету с зараженного компьютера есть вероятность отправки вирусом важной информации злоумышленникам или распространения вируса по адресам вашей адресной книги. Именно поэтому при подозрении на заражение лучше всего сразу отключиться от интернета.
 Запустите полную проверку компьютера

Профилактика заражения

Никакие самые надежные и разумные меры не смогут обеспечить стопроцентную защиту от компьютерных вирусов и троянских программ, но, выработав для себя ряд правил, вы существенно снизите вероятность вирусной атаки и степень возможного ущерба.

Одним из основных методов борьбы с вирусами является своевременная профилактика. Компьютерная профилактика состоит из небольшого количества правил, соблюдение которых значительно снижает вероятность заражения вирусом и потери каких-либо данных.

Ниже перечислены основные правила безопасности, выполнение которых позволит избегать вирусных атак.

Правило № 1: защитите компьютер с помощью антивирусных программ и программ безопасной работы в интернете. Для этого:

 Безотлагательно установите антивирусную программу.
 Регулярно обновляйте сигнатуры угроз, входящие в состав программы.

Правило № 2: будьте осторожны при записи новых данных на компьютер:

 Проверяйте на присутствие вирусов все съемные диски (дискеты, CD-диски, флеш-карты и пр.) перед их использованием.
 Осторожно обращайтесь с почтовыми сообщениями. Не запускайте никаких файлов, пришедших по почте, если вы не уверены, что они действительно должны были прийти к вам, даже если они отправлены вашими знакомыми.
 Внимательно относитесь к информации, получаемой из интернета. Если с какого-либо веб-сайта вам предлагается установить новую программу, обратите внимание на наличие у нее сертификата безопасности.
 Если вы копируете из интернета или локальной сети исполняемый файл, обязательно проверьте его с помощью антивирусной программы.
 Внимательно относитесь к выбору посещаемых вами интернет-ресурсов. Некоторые из сайтов заражены опасными скрипт-вирусами или интернет-червями.

Правило № 3: пользуйтесь сервисом Windows Update и регулярно устанавливайте обновления операционной системы Microsoft Windows.

Правило №4: покупайте дистрибутивные копии программного обеспечения у официальных продавцов.

Правило № 5: ограничьте круг людей, допущенных к работе на вашем компьютере.

Правило № 6: уменьшите риск неприятных последствий возможного заражения:

 Своевременно делайте резервное копирование данных.
 Создайте диск аварийного восстановления, с которого при необходимости можно будет загрузиться, используя "чистую" операционную систему.

Правило № 7: регулярно просматривайте список установленных программ на вашем компьютере. Для этого вы можете воспользоваться пунктом **Установка/удаление программ** в **Панели инструментов** или просто просмотреть содержимое каталога **Program Files**, каталога автозагрузки.

Основные антивирусные программы:

1. **Norton Antivirus**
2. **Dr. Web**
3. **Kaspersky Antivirus**
4. **NOD 32**
5. **Mc Afee**
6. **Panda Antivirus**

ПРИЛОЖЕНИЕ 2
УТВЕРЖДЕНО
Приказом директора школы
от 18.10.2012 № 69

Должностная инструкция лица ответственного за работу Интернета и внедрение системы контент- фильтрации в образовательном учреждении

Ответственный за работу Интернета и ограничение доступа назначается приказом руководителя образовательного учреждения. В качестве ответственного за организацию доступа к сети Интернет может быть назначен заместитель руководителя образовательного учреждения по учебно-воспитательной работе, учитель информатики, другой сотрудник образовательного учреждения.

1. Общие положения

Должен знать:
-дидактические возможности использования ресурсов сети Интернет;
-правила безопасного использования сети Интернет.

2. Должностные обязанности:

-планирует использование ресурсов сети Интернет в образовательном учреждении на основании заявок учителей и других работников образовательного учреждения;

-разрабатывает, согласует с педагогическим коллективом, представляет на педагогическом совете образовательного учреждения регламент использования сети Интернет в образовательном учреждении, включая регламент определения доступа к ресурсам сети Интернет;

-организует получение сотрудниками образовательного учреждения электронных адресов и паролей для работы в сети Интернет и информационной среде образовательного учреждения:

-организует контроль за использованием сети Интернет в образовательном учреждении;

-организует контроль за работой оборудования и программных средств, обеспечивающих использование сети Интернет и ограничение доступа;

систематически повышает свою профессиональную квалификацию, общепедагогическую и предметную компетентность, включая ИКТ- компетентность, компетентность в использовании возможностей Интернета в учебном процессе:

-обеспечивает информирование организаций. отвечающих за работу технических и программных средств, об ошибках в работе оборудования и программного обеспечения;

-соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети Интернет.

3. Права

Вправе определять ресурсы сети Интернет, используемые обучающимися в учебном процессе на основе запросов преподавателей и по согласованию с руководителем образовательного учреждения.

4. Ответственность

Несет ответственность за выполнение правил использования Интернета и ограничения доступа, установленного в образовательном учреждении.

4.1 Посещать сайты, содержание и тематика которых недопустимы для несовершеннолетних и (или) нарушают законодательство Российской Федерации (порнография, эротика, пропаганда насилия, терроризма, политического и религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности).

4.2 Загрузка и распространение материалов, содержащих 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 размещение ссылок на выше указанную информацию.

4.3 Загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.

4.4 Распространять информацию, порочащую честь и достоинство граждан.

4.5 Вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах.

4.6 Изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нем (заставки, картинку рабочего стола, стартовой страницы браузера).

4.7 Включать. выключать и перезагружать компьютер без согласования с ответственным за организацию в учреждении работы сети Интернет.

4.8 Осуществлять действия. направленные на «взлом» любых компьютеров, находящихся как в «точке доступа к Интернету» школы, так и за его пределами.

4.9 Использовать возможности «точки доступа к Интернету» учреждения для пересылки и записи непристойной, клеветнической, оскорбительной, угрожающей и порнографической продукции, материалов и информации.

4.10 Осуществлять любые сделки через Интернет.

4.11.Работать с объемными ресурсами (видео, аудио, чат, фото) без согласования с лицом, назначенным ответственным за организацию в учреждении работы сети Интернет.

4.12 Пользователи несут ответственность:

-За содержание передаваемой, принимаемой и печатаемой информации.

-За нанесение любого ущерба оборудованию в «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния) пользователь не сет материальную ответственность в соответствии с законодательством.

При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, учащийся обязан незамедлительно сообщить об этом преподавателю, проводящему занятие. Преподаватель обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом лицу, ответственному за работу сети и ограничение доступа к информационным ресурсам.

Пользователи имеют право:

- Работать в сети Интернет в течение периода времени, определенного Правилами учреждения.

- Сохранять полученную информацию на съемном диске.

- Размещать собственную информацию в сети Интернет на интернет- ресурсах учредения.

- Иметь учетную запись электронной почты на интернет-ресурсах учреждения.

ПРИЛОЖЕНИЕ 2
УТВЕРЖДЕНО
Приказом директора школы
от 28.10.2012 № 70

Принято:	Утверждаю:
на заседании педагогического совета	Директор школы: Н.М.Сополькова
Протокол № 2 от 28.10.2012	Приказ № 70 от 28.10.2012

Положение
о порядке обработки и обеспечении безопасности персональных данных в ОУ

1. Общие положения

Настоящее Положение разработано в соответствии с Федеральным законом «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и устанавливает единый порядок обработки персональных данных работников и обучающихся образовательного учреждения и гарантии их конфиденциальности.

В целях настоящего Положения используются следующие термины и понятия:

- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

- обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

- информационная система персональных данных (далее - ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

2. Основные условия обработки персональных данных

2.1. Обработка персональных данных обучающегося осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов в целях воспитания и обучения обучающегося, обеспечения его личной безопасности, контроля качества образования, пользования льготами, предусмотренными законодательством Российской Федерации и локальными актами администрации.

2.2. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, составленного по форме согласно приложению №1 или №2 к настоящему Положению, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона;

- после принятия необходимых мер по защите персональных данных.

2.3. Приказом директора назначается сотрудник, ответственный за защиту персональных данных работников и обучающихся ОУ, и определяется перечень лиц, допущенных к обработке персональных данных.

2.4. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации, содержащей персональные данные, по форме согласно приложению №3 к настоящему Положению.

2.5. Запрещается:

- обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;
- осуществлять ввод персональных данных под диктовку.

2.10. При передаче персональных данных лица, передающие персональные данные обязаны:

- предупредить лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены,
- потребовать от этих лиц письменное подтверждение соблюдения этого условия.

2.11. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных, определяются трудовыми договорами и должностными инструкциями.

2.12. Все сведения о передаче персональных данных регистрируются в Журнале учёта передачи персональных данных (по форме согласно приложению №6 к настоящему Положению) в целях контроля правомерности использования данной информации лицами, её получившими.

3. Условия обработки персональных данных обучающихся ОУ

3.1. Право доступа к персональным данным обучающихся ОУ имеют:

- работники департамента (управления) образования (при наличии соответствующих полномочий, установленных приказом департамента (управления) образования;
- директор образовательного учреждения;
- главный бухгалтер образовательного учреждения;
- заместитель директора по УВР,классные руководители (только к персональным данным обучающихся своего класса);
- ответственный за питание; библиотекарь;
- инспектор по охране прав детства; врач/медработник.

3.2. Директор образовательного учреждения может передавать персональные данные обучающегося третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья обучающегося, а также в случаях, установленных федеральными законами.

3.3. Секретарь: - принимает или оформляет вновь личное дело обучающегося и вносит в него необходимые данные;

- предоставляет свободный доступ родителям (законным представителям) к персональным данным обучающегося на основании письменного заявления. Не имеет права получать информацию об обучающемся родитель (законный представитель), лишенный или ограниченный в родительских правах на основании вступившего в законную силу постановления суда.

3.4. Главный бухгалтер имеет право доступа к персональным данным обучающегося в случае, когда исполнение им своих трудовых обязанностей или трудовых обязанностей работников бухгалтерии по отношению к обучающемуся (предоставление льгот, установленных законодательством) зависит от знания персональных данных обучающегося.

4. Порядок определения защищаемой информации

4.1. ОУ создает в пределах своих полномочий, установленных в соответствии с федеральными законами, ИСПДн в целях обеспечения реализации прав объектов персональных данных.
4.2. В ОУ на основании «Перечня сведений конфиденциального характера», утвержденного Указом Президента РФ от 06.031997 г. № 188, определяется и утверждается перечень сведений ограниченного доступа, не относящихся к государственной тайне (далее - конфиденциальной информации) и перечень информационных систем персональных данных.
4.3. На стадии проектирования каждой ИСПДн определяются цели и содержание обработки персональных данных, утверждается перечень обрабатываемых персональных данных.

5. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

5.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства РФ от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.
5.2. Оператором осуществляется классификация информационных систем персональных данных в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 г. № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" в зависимости от категории обрабатываемых данных и их количества.
5.3. Мероприятия по обеспечению безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с приказом ФСТЭК России от 05.02.2010 г. №58 «О методах и способах защиты информации в информационных системах персональных данных».
5.4. Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации при отсутствии:
- утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации ИСПДн, инструкции пользователя, администратора по организации антивирусной защиты, и других нормативных и методических документов;
- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;
- охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

6. Порядок обработки персональных данных без использования средств автоматизации

6.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде

документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.
6.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.
6.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

6.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.5. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.
6.6. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.
6.7. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению №3 к настоящему Положению.
К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.
6.8. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других

зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

6.9. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

6.10. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

7. Ответственность должностных лиц

7.1. Работники, допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

ПРИЛОЖЕНИЕ 2
УТВЕРЖДЕНО
Приказом директора школы
от 28.10.2012 № 70

Принято:	Утверждаю:
на заседании педагогического совета	Директор школы: Н.М.Сополькова
Протокол № 2 от 28.10.2012	Приказ № 70 от 28.10.2012

ПОЛОЖЕНИЕ
об информационном узле (сайте) Муниципального казенного общеобразовательного учреждения «Миниская основная общеобразовательная школа»

1. Общие положения
1.1. Настоящее Положение определяет назначение, принципы построения и структуру информационных материалов, размещаемых на официальном информационном узле (сайте) Муниципального казенного общеобразовательного учреждения «Миниская основная общеобразовательная школа » (далее – Сайт), а также регламентирует технологию их создания и функционирования.
1.2. Сайт обеспечивает официальное представление информации о школе в сети Интернет с целью расширения рынка образовательных услуг школы, оперативного ознакомления преподавателей, работников, обучающихся, родителей, деловых партнеров и других заинтересованных лиц с образовательной деятельностью школы.
1.3. Пользователем Сайта может быть любое лицо, имеющее технические возможности выхода в Интернет.
Функционирование Сайта регламентируется действующим законодательством, уставом школы, настоящим Положением.
Настоящее Положение может быть изменено и дополнено в соответствии с приказом директора школы.

2. Информационный ресурс Сайта
2.1. Информационный ресурс Сайта формируется в соответствии с деятельностью всех структурных подразделений школы, ее преподавателей, работников, обучающихся, родителей, деловых партнеров и прочих заинтересованных лиц.
2.2. Информационный ресурс Сайта является открытым и общедоступным.
2.3. Условия размещения ресурсов ограниченного доступа регулируются отдельными документами; размещение таких ресурсов допустимо только при наличии соответствующих организационных и программно-технических возможностей.
2.4. Основными информационно-ресурсными компонентами Сайта являются:
- общая информация о школе, как муниципальном общеобразовательном учреждении города,
- справочные материалы об образовательных программах, порядке поступления в школу;
- материалы по организации учебного процесса;
- учебно-методические материалы преподавателей школы;
- материалы о научно-исследовательской деятельности обучающихся и их участии в олимпиадах и конкурсах;
- электронные каталоги информационных ресурсов школы;

- подборки тематических материалов по изучаемым в школе профилям;
- материалы о персоналиях — руководителях, преподавателях, работниках, выпускниках, деловых партнерах и т. п.;
- материалы о событиях текущей жизни школы, проводимых в школе и при ее участии мероприятиях, архивы новостей;
- информация об обновлении содержания разделов Сайта с указанием даты обновления, названия раздела и аннотации к обновленной информации.
2.5. Размещение информации рекламно-коммерческого характера допускается только по согласованию с директором школы. Условия размещения такой информации регламентируются специальными договорами
2.6. Часть информационного ресурса, формируемого по инициативе подразделений, творческих коллективов, педагогов и обучающихся школы, может быть размещена на отдельных специализированных сайтах, доступ к которым организуется с Сайта школы.

3. Организация информационного наполнения и сопровождения Сайта
3.1. Информационное наполнение и актуализация Сайта осуществляется совместными усилиями директора школы, заместителей директора, методических объединений, структурных подразделений и общественных организаций школы.
3.2. По каждому разделу Сайта (информационно-ресурсному компоненту) определяются подразделения (должностные лица), ответственные за подборку и предоставление соответствующей информации. Перечень обязательно предоставляемой информации и возникающих в связи с этим зон ответственности подразделений утверждается директором школы.
3.3. Руководство обеспечением функционирования Сайта и его программно-технической поддержкой возлагается на заместителя директора школы, ответственного за информатизацию образовательного процесса.
3.4. Заместитель директора школы, ответственный за информатизацию образовательного процесса, обеспечивает качественное выполнение всех видов работ, непосредственно связанных с эксплуатацией Сайта: изменение дизайна и структуры, размещение новой и удаление устаревшей информации, публикация информации из баз данных, разработка новых web-страниц, реализация политики разграничения доступа и обеспечение безопасности информационных ресурсов.
3.5. Заместитель директора школы, ответственный за информатизацию образовательного процесса, осуществляет консультирование лиц, ответственных за предоставление информации, по реализации концептуальных решений и текущим проблемам, связанным с информационным наполнением и актуализацией информационного ресурса.
3.6. Непосредственное выполнение работ по размещению информации на Сайте, обеспечению ее целостности и доступности, реализации правил разграничения доступа возлагается на администратора Сайта (далее – Администратор), который назначается директором школы и подчиняется заместителю директора школы, ответственному за информатизацию образовательного процесса.
3.7. Информация, готовая для размещения на Сайте, предоставляется в электрон-ном виде Администратору, который оперативно обеспечивает ее размещение в соответствующем разделе Сайта. Текстовая информация предоставляется в формате doc, графическая – в формате jpeg или gif.
3.8. В порядке исключения текстовая информация может быть предоставлена в рукописном виде без ошибок и исправлений, графическая – в виде фотографий, схем, чертежей – в этом случае перевод в электронный вид осуществляется под руководством заместителя директора школы, ответственного за информатизацию образовательного процесса. Порядок исключения определяет директор школы
3.9. В случае устаревания информации, относящейся к подразделению, обновленная информация должна быть предоставлена Администратору не позднее трех дней после

внесения изменений.
3.10. Текущие изменения структуры Сайта осуществляются Администратором по согласованию с заместителем директора школы, ответственным за информатизацию образовательного процесса. Изменения, носящие концептуальный характер, согласовываются с директором школы.

4. Ответственность
4.1. Ответственность за недостоверное, несвоевременное или некачественное предоставление информации (в т.ч. с грамматическими или синтаксическими ошибка-ми) для размещения на Сайте несет руководитель соответствующего подразделения (должностное лицо).
4.2. Ответственность за некачественное текущее сопровождение Сайта несет Администратор. Некачественное текущее сопровождение может выражаться:
- в несвоевременном размещении предоставляемой информации;
- в совершении действий, повлекших причинение вреда информационному ресурсу;
- в невыполнении необходимых программно-технических мер по обеспечению целостности и доступности информационного ресурса.
4.3. Ответственность за нарушение работоспособности и актуализации Сайта вследствие реализованных некачественных концептуальных решений, отсутствия четкого порядка в работе лиц, на которых возложено предоставление информации, несет заместитель директора школы, ответственный за информатизацию образовательного процесса школы