Приложение № 1
к приказу № 394 от 02.08.2018 г.

«Утверждаю»
Директор МАОУ «СОШ № 36
г. Челябинска»
М.Б. Меньшенина

ПОЛОЖЕНИЕ
об ответственных лицах за функционирование контентной фильтрации доступа к сети Интернет в МАОУ «СОШ № 36 г. Челябинска».

1. Общие положения.

1.1. Настоящее Положение разработано для урегулирования условий и порядка применения ресурсов сети Интернет обучающимися и сотрудниками МАОУ «СОШ № 36 г. Челябинска» в соответствии с Федеральным законом Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", Федеральным законом Российской Федерации от 21июня 2011 г. N 252-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», статьями 15.1, 15.2 и 15.3 Федерального закона от 27 июля 2006 года Н2149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности».

1.2. Использование сети Интернет в МАОУ «СОШ № 36 г. Челябинска» подчинено следующим принципам:

1.2.1. соответствие образовательным целям;

1.2.2. содействия гармоничному формированию и развитию личности;

1.2.3.уважения закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;

1.2.4.приобретения новых навыков и знаний;

1.2.5.расширения применяемого спектра учебных и наглядных пособий;

1.2.6. социализации личности, введения в информационное общество.

2. Организация и контроль использования сети Интернет в МАОУ «СОШ № 36 г. Челябинска»

2.1. Приказом директора МАОУ «СОШ № 36 г. Челябинска»назначается ответственный за работу в сети Интернет и ограничение доступа. В качестве ответственного за организацию доступа к сети Интернет может быть назначен заместитель директора по учебно-воспитательной работе, заместитель директора по ИКТ, преподаватель информатики, другой сотрудник МАОУ «СОШ № 36 г. Челябинска».

2.2. В МАОУ «СОШ № 36 г. Челябинска» приказом директора

утверждаются и вводятся в действие следующие локальные акты:

• настоящее Положение об ответственных лицах за функционирования средств контентной фильтрации доступа к сети Интернет в МАОУ «СОШ № 36 г. Челябинска»;

• инструкция для сотрудников МАОУ «СОШ № 36 г. Челябинска» о порядке действий при осуществлении контроля использования обучающимися сети Интернет;

• правила использования сети Интернет в МАОУ «СОШ № 36 г. Челябинска»;

• классификатор информации, не имеющей отношения к образовательному процессу.

2.3. Приказом директора МАОУ «СОШ № 36 г. Челябинска» создается комиссия по проверке работоспособности школьной системы контент-фильтрации (не менее 4-х человек вместе с председателем). Не реже 1 раза в месяц комиссия должна проверять:

2.3.1. работоспособность системы контент-фильтрации (далее-СКФ) на всех компьютерах учреждения путем ввода в поле поиска любой поисковой системы ключевых слов из списка информации, запрещенной для просмотра учащимися, с последующими попытками загрузки сайтов из найденных. Необходимо, в том числе, проверить загружается ли информация, причиняющая вред здоровью и развитию детей, не имеющая отношения к образовательному процессу, в социальных сетях: «В контакте», «Одноклассники», twitter.com, facebook.com , Живой Журналalivejournal.com и т.д.;

2.3.2. работоспособность журнала, фиксирующего адреса сайтов, посещаемых с компьютеров школы. По итогам проверки составляется акт, который подписывается всеми членами комиссии. При выявлении компьютеров, подключенных к сети Интернет и не имеющих СКФ, производятся одно из следующих действий:

•немедленная установка и настройка СКФ;

•немедленное программное и/или физическое отключение доступа к сети Интернет на выявленных компьютерах;

2.3.3. установить последние обновления операционной системы Windows (http://windowsupdate.microsoft.com);

2.3.4. включить режим автоматической загрузки обновлений. (Пуск -> Настройка -> панель управления -> Автоматическое обновление -> Автоматически загружать и устанавливать на компьютер рекомендуемые обновления);

2.3.5.скачать с сайта www.microsoft.com программное обеспечение WindowsDefender и установить на все компьютеры. Включить режим автоматической проверки. Включать режим проверки по расписанию каждый день;

2.3.6. активировать встроенный брандмауэр Windows (Пуск -> Настройка -> панель управления -> Брандмауэр Windows -> Включить);

2.3.7. установить антивирусное программное обеспечение на каждый компьютер. Включить режим автоматического сканирования файловой системы. Включить режим ежедневной автоматической проверки всей файловой системы при включении компьютера. Активировать функцию ежедневного автоматического обновления антивирусных баз;

2.3.8. Ежедневно проверять состояние антивирусного программного обеспечения, а именно:

a. режим автоматической защиты должен быть включен постоянно;

b. дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты;

c. просматривать журналы ежедневных антивирусных проверок. Контролировать удаление вирусов при их появлении;

2.3.9. не реже одного раза в месяц посещать сайт hhttp://windowsupdate.microsoft.com и проверять установлены ли последние обновления операционной системы;

2.3.10. быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы;

2.3.11. контролировать посещение Интернет-сайтов пользователями. Не допускать посещения т.н. "хакерских", порно и других сайтов с потенциально вредоносным содержанием.

2.3.12. в обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними;

2.3.13. при появлении признаков нестандартной работы компьютера ("тормозит", на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от Ethernet сети, загрузить компьютер с внешнего загрузочного диска (CD, DVD) и произвести полную антивирусную проверку всех дисков компьютера. При появлении аналогичных признаков после проделанной процедуры переустановить операционную систему с форматированием системного раздела диска.