

Согласовано
Председатель профкома
_____И.З.Ахкамова
« 4 » апреля 2014 г.

Утверждаю
Директор МОБУ СОШ №1
_____Р.Ф. Шайбакова
« 4 » апреля 2014 г.

ИНСТРУКЦИЯ **по организации внедрения системы контентной фильтрации в образовательном учреждении**

ОБЩИЕ ПОЛОЖЕНИЯ

Для защиты от нецелевого использования интернет-ресурсов разработаны программные средства, использующие технологию URL. Фильтрация трафика по контенту (содержимому) позволяет блокировать непродуктивную и незаконную деятельность сотрудников в сети Интернет, регулировать пропускную способность сетевых каналов, назначая квоты для пользователей и блокируя протоколы приложений, интенсивно потребляющих трафик.

В данном документе рассмотрены действия, которые должны быть проведены должностными лицами при внедрении системы контентной фильтрации (СКФ) в образовательных учреждениях. Рассмотрены действия:

- Ответственных за внедрение системы контентной фильтрации в образовательном учреждении.

Внедрение системы контентной фильтрации требует от должностных лиц проведения следующих мероприятий:

- Ввод в систему информации об образовательных учреждениях более низкого уровня;
- Регистрация Администраторов для подчиненных учреждений;
- Передача входных учетных записей зарегистрированным Администраторам;
- Получение программного обеспечения фильтрации и установка его на соответствующие рабочие станции;

Основной задачей Администраторов системы СКФ в школах является установка и обслуживание программного обеспечения фильтрации - Персонального клиентского фильтра (ПКФ). Для этого необходимо скачать с сайта СПП дистрибутив ПКФ и "Руководство оператора ПКФ". После ознакомления с "Руководством оператора ПКФ" Администратор должен установить программное обеспечение на рабочие станции своей школы. После получения уведомления от уже установленного клиентского приложения о наличии на сайте новой версии дистрибутива необходимо повторить процедуру загрузки и установки ПО. Установленное программное обеспечение (ПКФ) необходимо проверить на работоспособность путем попытки зайти с компьютера, где оно установлено на два сайта: <http://www.sovsport.ru/> - доступ должен быть разрешен; <http://boobs.ru/> - доступ должен быть запрещен.

Для осуществления этих действий ответственным лицам необходимо авторизоваться на сайте <http://skf.edu.ru>. Данные авторизации должны быть получены от вышестоящей организации. После успешной авторизации будут доступны следующие разделы:

- "Категории" - управление регламентом доступа к категориям Интернет-ресурсов. В данном разделе перечислены категории Интернет-ресурсов, входящие в общий Классификатор информации запрещенной законодательством Российской Федерации к распространению.
- "Методические указания" - просмотр размещенных документов на сайте СПП
- "Скачать дистрибутив" - получение последней версии дистрибутива ПКФ.
- "Личные данные" - просмотр и редактирование личных данных ответственного лица.

- "Клиент" - просмотра и редактирования списка подчиненных организаций (клиентов СКФ).

При работе с веб-ресурсами:

1. Пользователи используют программы для поиска информации в WWW только в случае, если это необходимо для выполнения задач, связанных с образованием и воспитанием.
2. Использование ресурсы сети Интернет разрешается только в учебных целях, использование её ресурсов не должно потенциально угрожать образовательному учреждению.
3. По использованию Интернет ведется статистика заведующим кабинетом.
4. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротocolированы и использоваться для принятия решения о применении к нему санкций.
5. Сотрудникам организации, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским и не относящимся к деятельности образовательного учреждения.
6. На все компьютеры, используемые для доступа к сети Internet, сетевым администратором должна быть настроена система контентной фильтрации.
7. Все файлы, загружаемые с помощью сети Internet, должны проверяться на вирусы с помощью антивирусных программ.
8. Сотрудники, нанятые по контракту, должны соблюдать эту политику после предоставления им доступа к Internet. Доступ к сети Internet предоставляется по согласованию с заведующим кабинета.
9. В организации должен вестись список запрещенных сайтов. Программы для работы с Internet должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.
10. Запрещено размещать в гостевых книгах, форумах, конференциях сообщения, содержащие грубые и оскорбительные выражения.
11. Запрещено получать и передавать через СЕТЬ информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.
12. Запрещено получать доступ к информационным ресурсам СЕТИ или сети Интернет, не являющихся публичными, без разрешения их собственника.