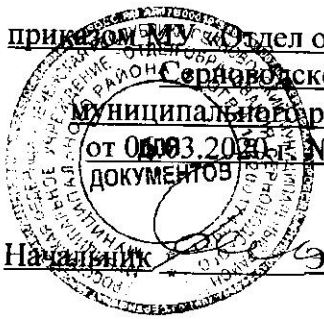
УТВЕРЖДЕНО

приказом МУ «Отдел образования Серноводского муниципального района» от 01.03.2013 г. №27-п



Начальник Э.А. Улубаев

ПОЛОЖЕНИЕ
об организации безопасного управления контентом в ОУ Серноводского муниципального района

Настоящее положение разработано с целью организации работы по защите обучающихся от доступа к информации, не совместимой с задачами образовательного учреждения.

Для защиты обучающихся от информации, не совместимой с задачами учреждения требуется применение система безопасного управления контентом, или, Secure Content Management (SCM) - это система, которая должна обеспечивать контроль за содержанием потоков информации, передаваемых и получаемых организацией из Сети. SCM-система должна обеспечивать управление контентом на базе определенных политик, проводимых организацией, и обычно включает управление Web-контентом, контроль за обменом сообщениями, защиту от вирусов и нежелательных, скачиваемых из Сети приложений.

Обычно выделяются следующие SCM-подсистемы:

- Employee Internet Management (EIM) — контроль доступа сотрудников (учащихся) в Интернет;
- Internet Application Security (IAS) — контроль проникновения нелегального контента в сеть организации;
- E-mail scan (ES) — контроль утечки приватной информации из сети организации и фильтрация спама;
- Virus scan (VS) — контроль проникновения вирусов.

Обозначенная тема раскрывается (например) в следующих статьях: "Как сэкономить на Web-трафике сотрудников", Автор: Александр Прохоров http://www.compress.ru/Archive/CP/2005/11/12/.

Для ограничения нецелевого использования Интернета на рабочих местах существует целый ряд технических решений как отечественного, так и западного производства:

- Proventia Web Filter (Технология, положенная в основу данного продукта, была приобретена у компании Cobion) — это блокиратор нежелательного Web-содержимого, который ежемесячно анализирует 120 млн. Web-страниц и ежедневно добавляет в базу 100 тыс. новых и обновленных Web-страниц.
- CS MIMEsweeper for Web — средство контроля и разграничения доступа к Web, обеспечивающее в том числе защиту от утечки конфиденциальных материалов через бесплатные Интернет-сервисы — Web-почту, чаты и доски объявлений. Эта программа защищает от распространения вирусов через Web, от запрещенного

серфинга, от нецелевых скачиваний и помещения нелегальной информации на внешние Web-ресурсы.

• SurfControl Web Filter — средство управления доступом в Интернет в корпоративных сетях. Программа предоставляет доступ к полезной информации в Интернете, одновременно преграждая доступ к Web-сайтам, не относящимся к их деятельности. Кроме того, вероятность потери важных данных или выхода из строя всей сети может быть снижена за счет запрещения загрузки потенциально опасных файлов, которые могут содержать вирусы либо другой разрушительный или опасный программный код (файлы *.doc, *.vbs, *.elm, *.exe и *.zip).

• Webwasher URL Filter резко сокращает нецелевое использование Web-ресурсов за счет блокировки определенных категорий сайтов, например, из разделов Shopping и Entertainment. Система также предотвращает возможность скачивания файлов определенных расширений, в частности MP3.

Безопасность контента

Системы контроля безопасности контента в первую очередь призваны осуществлять контроль за содержанием потоков информации, передаваемых в Интернет и получаемых из Сети в локальную. К задачам систем контент-секьюрити относятся также проверка информации, хранящейся в локальной сети, контроль за содержанием корпоративной электронной почты, а также контроль за просматриваемой информацией с целью предотвращения использования Интернета в личных целях.

Необходимость систем контент-секьюрити диктуется тем, что Интернет — это источник информации, за который никто не несет ответственности, и вероятность получения из него недостоверной, оскорбительной, пиратской или запрещенной по другим причинам информации весьма велика.

Проблема скачивания вредоносного контента.

Интернет является мощным инструментом обучения. Однако помимо полезной информации в Интернете ученики могут встретиться с нежелательным контентом.

Последний можно разделить на две группы:

1. запрещенный контент для любого возраста
2. нежелательный для детей и подростков.

К ресурсам первого рода относятся:

1. сайты с детской порнографией,
2. сайты террористов,
3. сайты разжигающие расовую дискриминацию и т.п.

Наличие во внутренней сети учебного заведения подобной информации может вызвать не только претензии к ученикам, которые подобный контент скачивают на рабочую станцию сети, но и к уголовному преследованию администрации, которая допускает хранение подобных материалов.

К сайтам нежелательным для детей (кроме уже упомянутых) относятся сайты, которые дети не должны посещать по возрастным ограничениям:

- жестокие игры
- онлайновые казино
- порнография
- сайты, пропагандирующие насилие
- сайты сексуальных меньшинств

- сайты магазинов интим-услуг и т.п.

Нежелательным контентом может являться также тот, который отвлекает детей от учебного процесса. Дети могут вместо выполнения учебного задания в Сети, заниматься просмотром материалов разрешенного характера, но не имеющего ничего общего с учебным процессом.

Проблема утечки контента из учебного заведения

В учебном заведении возможна проблема проникновения нежелательного контента внутрь учебной сети, также возможна проблема утечки контента. В данном случае, во-первых, речь идет об утечке приватных персональных данных. В современном обществе существует проблема похищения детей, сексуальные домогательства и проч. Поэтому личная информация о ребенке (его фотография, расписание уроков, e-mail, телефон) не должны вывешиваться в Сети для свободного доступа.

При размещении фотографий в Сети (например, на школьном Web-сайте) желательно размещать фотографии детей только с согласия родителей, и только групповые. Не стоит указывать имена детей и другую личную информацию.

Вторая проблема — это рассылка по почте или размещение на школьном (или другом) сайте запрещенного контента. Рассылка пиратского ПО, порнографии и т.п.

Трафикоемкие (объемные) процедуры доступа к информации.

Трафикоемкие процедуры - скачивание видеофильмов, музыки, файловых архивов программного обеспечения ведут к резкому увеличению трафика, что может замедлять работу сети и увеличивать расходы на оплату трафика. Большинство программ, которые блокируют доступ у запрещенным Web-сайтам обеспечивают и контроль трафикоемких процедур.

Варианты проникновения/утечки контента.

Нежелательный контент попадает в сеть учебного заведения преимущественно по двум каналам: через Web-трафик и через почтовый трафик.

Проблема фильтрации почтового трафика широко известна как проблема спама. В качестве спама могут распространяться сообщения оскорбительного характера, призывы к насилию и т.п. Помимо всех вышеперечисленных проблем с наличием нежелательного контента в письмах спам генерирует лишний трафик, отвлекает пользователей.

Конечно, возможно попадание подобного контента также с flash-накопителей, CD, DVD дисков.

Борьба с нежелательным контентом.

Следует предпринять организационные и технические меры.

Организационные меры - назначение ответственных лиц, режим доступа в компьютерный класс, доведение до сведения учащихся норм поведения в Сети, ответственности за противоправные действия и т.п.), технические меры-фильтрация трафика, мониторинг действий учащихся.

Наличие мониторинга (даже без фильтрации) уже может стать эффективной мерой. Если ученик будет знать, что за его действиями (всеми посещениями ведется постоянный мониторинг и все его действия записываются в log-файлах с указанием того, кто, когда и что посещал) то это уже в существенной мере ограничит вероятность посещения нежелательных сайтов.

Варианты фильтрации контента.

Контент может фильтроваться на уровне провайдера, на уровне шлюза в Интернет защищаемой сети и на уровне клиентской станции.

Фильтрация может быть построена на основе внешней обновляемой базы данных запрещенных ресурсов и может быть построена на основе локальной программы, которая действует по собственным принципам фильтрации («черные», «белые» списки, ключевые слова и т.п.).

При этом в принципе фильтрация может быть построена по принципу:

1. «Запрещаем все, кроме того, что можно»
2. «Можно все, кроме того, что запрещено»

Конечно, реализовать фильтрацию по принципу «Запрещаем все, кроме того, что можно» построить достаточно просто, подобная форма, возможно, имеет смысл для младших школьников, но в этом случае Интернет теряет многие свои функции.

Второй вариант требует построения и обновления огромной базы данных (поддерживать ее должен провайдер сервиса), которая постоянно пополняет базу запрещенного контента.

Для полноценной реализации второго вида фильтрации необходимо проиндексировать миллиарды Web-страниц и это под силу только крупным провайдерам подобного сервиса, например, таким как ISS. В частности, по такому принципу работает Proventia Web Filter, о которой будет сказано ниже. Чем больше база, тем качественнее и дороже решение.

Сложности фильтрации контента в школах.

Каждый день в Интернете появляются тысячи новых сайтов, поэтому, даже используя обновления баз данных с нежелательными ресурсами, добиться 100%-ной фильтрации невозможно. Отдельная проблема это недостаточная фильтрация русскоязычного контента западными продуктами. Возможны ошибки, когда фильтр будет отсеивать сайты полезного содержания. В общем, чем более интеллектуален фильтр, и чем больше база, на которую он опирается, тем дороже решение и тем оно менее доступно для школ.

Администраторы в школах имеют различный опыт работы с компьютерами и даже непрофессионал должен иметь возможность создавать и поддерживать политику фильтрации. Образовательный процесс включает множество различных областей науки и фильтрация должна быть всеобъемлющей, настраиваемой, а также обеспечивать защиту от новейших угроз.

Мониторинг Интернет-активности.

Мониторинг и протоколирование — это во многих случаях первый и важнейший шаг в контролировании интернет доступа. Данная функция наглядно показывает серфинг-профиль пользователя. Учитель должен проверить, где находился ученик, что просматривал, в какое время и как долго.

Мониторинг дает быструю и точную картину Web серфинга. Данные об интернет активности защищены криптографически и хранятся в недоступном для неавторизованного просмотра виде. Любой посещенный ресурс может быть просмотрен, и впоследствии добавлен в список разрешенных или запрещенных листов.

Отчеты мониторинга (Monitoring Reports) четко показывают, какие Web-страницы посещались, время визита, Web-адрес, и прочая информация.

Фильтрация сетевого контента - системы позволяющие ограничивать доступ к тем или иным сетевым сервисам или сайтам.

Система CyberPatrol.

Фильтры системы CyberPatrol позволяют учителям контролировать как, когда и кому интернет-доступ разрешен, (разрешен с ограничением (в виде фильтрации контента) или заблокирован в принципе).

- Фильтрация или блокирование web-сайтов, групп новостей и результатов, которые выдают поисковые машины, базируются на базе данных (категории CyberLIST), которая может донастраиваться путем добавления ваших собственных запрещенных или разрешенных сайтов или списков сайтов.
- Программа позволяет блокировать чаты и программы класса Instant Messaging
- Чат-сессии могут быть также подвергнуты фильтрации для предотвращения утечки важной информации, (имена, адреса телефоны и т.п.).

Программа поддерживает Лист разрешенных сайтов (YES List), который ограничивает пользователей серфингом только по заранее заданному разрешенному списку сайтов. Это хорошее решение для младших школьников.

- Программа предоставляет возможность выбирать заранее заданные настройки (Preset Filter Strengths). Имеются группы Ребенок (Child), Младшие тинэйджеры (Young Teen), Старшие тинэйджеры (Mature Teen) и т.п.
- Имеется также возможность настроить профиль фильтрации, указав какие категории сайтов должны фильтроваться жестко, а какие мягко.
- Еженедельные листы обновлений (Weekly List Updates) поступают еженедельно (или 2 раза в неделю), добавляя тысячи новых сайтов.
- CyberPatrol поставляется с функцией «ready-to-go filtering» (преднастроенной фильтрацией). Настройки могут быть изменены пользователем.
- Защита приватности предотвращает утечку приватной информации (имена /адрес/номер телефона). Информация фильтруется, прежде чем покинуть ваш компьютер.
- Доступны ограничения на время, проведенное в онлайне и доступ к определенным программам. Временной контроль позволяет ограничить длительное пребывание за компьютером, например, исключить длительное участие в сетевой игре.

Ограничения могут базироваться на времени суток (например, во время уроков), по дням недели и т.п.

Возможен контроль за скачиванием программ из Сети, поскольку скачивание программ из Сети может быть небезопасным, нарушать политику школы в отношении пользования пиратским ПО. Вы можете заблокировать скачивание без разрешения игр, музыки, графических файлов, видео. Это в свою очередь снизит риск загрузки шпионского ПО вирусов, скачивание пиратской продукции.

CyberPatrol использует многослойную защиту, которая включает следующие технологии:

1. CyberLIST – постоянно пополняемая база запрещенных сайтов.
2. CyberPATTERNS - технология контекстной фильтрация по ключевым словам (динамическая категоризация URL).

3. Web Page Analysis – контентный анализ Web-страниц на базе динамического посещения сайтов, которые еще не были категоризированы с помощью CyberLIST.
4. Web Link Analysis – на базе анализа Web-ссылок блокируются изображения непристойного содержания, которые могут возвращаться в ответ на запросы, не содержащие запрещенных ключевых слов.

Мощность Web-фильтрации может варьироваться за счет подключенных методов фильтрации.

Система Голкипер.

Голкипер 1.0 – Российская система контентной фильтрации, использующая эффективные алгоритмы работы и настроенная на русскоязычный контент. Программа, в первую очередь, предназначена для нужд Российских воспитательных и образовательных учреждений, а также организаций, обеспечивающих публичный доступ в Интернет.

Возможности Голкипера.

Работа с ресурсами на русском и иностранных языках: Наравне с отличной способностью анализировать русскоязычный контент, Голкипер также работает с другими основными языками мира, распределяя ресурсы по 48 категориям, которые охватывают более 200 тем.

Отчеты о доступе пользователей: Различные типы отчетов позволяют получить детальную статистику об использовании Интернет от детализированного отчета по сайту до общих отчетов об активности использования Интернет.

Модуль сбора и обработки статистики: Голкипер представляет уникальный инструмент для сбора и представления статистики в больших территориально-распределенных организациях с помощью специализированного модуля сбора и обработки статистики обращений пользователей, собираемых локальными контентными фильтрами, установленными в удаленных подразделениях организации.

Автоматическое обновление базы URL: Голкипер избавляет от дополнительной работы по обслуживанию, производя автоматическое обновление базы URL, списка категорий и других параметров.

Контентная фильтрация почтового трафика на уровне сети Электронная почта является одним из главных Интернет-сервисов (ежедневно в мире отправляется десятки млрд. электронных посланий) и одновременно является источником многочисленных проблем: спам, вирусы, распространение запрещенной информации.

Спамеры пытаются обмануть фильтры, придумывают новые формы сообщений, невидимые для фильтров, в надежде сохранить свой бизнес. В результате идет эволюция спам-фильтров, и параллельно эволюционируют средства доставки спама, а оплачивается этот процесс на деньги, получаемые от e-mail-пользователей.

Проблема состоит еще и в том, что спам тоже разнороден: одни сообщения представляют угрозу заражения вирусами и троянцами, другие просто отвлекают пользователей, поскольку маскируются под важные для них сообщения, третьи, не выдаваемые за что-то другое, не отнимают у получателей много времени.

Таким образом, антиспам — решение (как и антивирус) нельзя создать раз и навсегда — это результат непрерывного процесса накапливания сведений о спаме, его анализа и модернизации улавливающих его фильтров.

Система Proventia Mail Filter.

Proventia Mail Filter — это наиболее полное средство антиспама и фильтрации электронной почты, которое позволяет повысить производительность работы, освобождает ресурсы сети и защищает конфиденциальную информацию. Proventia Mail Filter анализирует входящую и исходящую почту для полной защиты от спама и утечки информации. Кроме спама, программа блокирует вирусы, порнографию и MP3-файлы.

Наиболее совершенные средства анализа в Proventia Mail Filter сочетаются с базой из более чем 200 тыс. наиболее распространенных примеров спама. Продукт не допускает блокирования нужных писем благодаря использованию 10-ступенчатого анализа письма, включая сравнение сообщения с базой спама и сравнение URL в e-mail-сообщениях с адресами Web-сайтов, занесенными в базу.

Процесс 10-ступенчатого анализа Proventia Mail Filter значительно превосходит аналоги, такие как включение в «черный» список и поиск по ключевым словам. Функция Proventia Mail Filter Spam Learn постоянно обновляет базу, которая четыре раза в день рассылает обновления конечным пользователям для обеспечения защиты в реальном времени.

Proventia Mail Filter анализирует исходящие e-mail-сообщения и блокирует письма с нежелательным содержимым, сохраняя интеллектуальную собственность и конфиденциальные документы. Программа анализирует текст сообщения, изображения и вложенные документы независимо от формата. Кроме того, она позволяет создавать специальные почтовые политики, устанавливать правила для входящих и исходящих e-mail.

Система персонального клиента фильтрации (ПКФ).

ПКФ разработан для работы в операционных системах Windows XP Home, Windows XP Pro, Windows 2000 Work Station, Windows 2003. При функционировании ПКФ происходит интеграция данного программного средства в операционную систему на уровне стека протоколов.

ПКФ был тщательно протестирован на возможность совместной работы с прикладными программными средствами различной конфигурации (например, с антивирусами и программным обеспечением типа «firewall»), однако в некоторых случаях возможно возникновение отдельных проблем в процессе инсталляции ПКФ, обусловленное многообразием видов и версий программного обеспечения, установленного на компьютерах пользователей.

В настоящее время нам известно о возможности возникновения на некоторых компьютерах следующих проблем:

1) прекращение работоспособности браузера Opera при установленном антивирусе Nod32;

В этом случае следует восстановить работоспособность браузера путем изменения настроек. Для этого:

а) выберите в меню пункт «Инструменты»;

б) выберите в меню пункт «Настройки»;

в) в открывшемся окне перейдите на закладку «Дополнительно»;

г) в подменю «Безопасность» отмените выбор пункта «Включить проверку мошенничества».

2) замедление работы компьютера при активированном антивирусе Norton Antivirus 2004;

В этом случае следует восстановить скорость работы отключением монитора антивируса на весь этап инсталляции ПКФ, включая необходимую перезагрузку и первичный запуск ПКФ.

Порядок установки ПКФ

1. Проверить компьютер программой антивирусом на отсутствие вирусов.
2. Создать точку восстановления. В Windows XP, например, это можно сделать, нажав кнопку «Пуск» на панели задач и затем выбирая «Программы» - «Стандартные» - «Служебные» - «Восстановление системы». Будет запущен мастер, которому следует указать «Создать точку восстановления», после чего следовать его указаниям.
3. Если после инсталляции ПКФ возникли проблемы, препятствующие нормальной работе с данным программным средством, нужно деинсталлировать ПКФ, перезагрузив компьютер в защищенном режиме.
4. В качестве программы для деинсталляции ПКФ может служить «System Mechanic 7 Professional», ограниченную по времени действия версию которой можно загрузить по адресу http://www.iolo.com/sm/7/pro/download.aspx.

Во избежание потери данных или нарушения режима корректной работы программного обеспечения данную операцию рекомендуется выполнять только опытным пользователям персональных компьютеров.

В настоящее время разработчики системы контентной фильтрации заняты решением известных проблем.

При обнаружении каких-либо недостатков или проблем в работе средств фильтрации Интернет-контента просим сообщать об этом по адресу support@cair.ru.

Порядок внедрения системы контентной фильтрации в образовательных учреждениях

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

- Ответственных за внедрение системы контентной фильтрации на уровне Управления Образования субъекта федерации;
- Ответственных за внедрение системы контентной фильтрации на муниципальном уровне;
- 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;
- Просмотр и изменение Классификатора информации запрещенной законодательством Российской Федерации к распространению для соответствующего субъекта федерации.
- Получение методической и технической документации с Сервера поддержки пользователей (СПП) Системы контентной фильтрации.

В общем виде методика внедрения сводится к последовательной делегации и передачи прав с верхнего на нижний уровень. Особенности использования СПП для выполнения соответствующих функций описаны в "Руководстве оператора СПП".

Перед началом работы ответственному лицу Отдела образования субъекта федерации необходимо создать подчиненные ему образовательные учреждения муниципального уровня, а в случае целесообразности и непосредственно школы. И определить в системе учетные записи для людей, ответственных за установку и поддержание в рабочем состоянии системы фильтрации на соответствующих уровнях. Регистрационные данные указанных ответственных лиц необходимо передать в Муниципальные образовательные учреждения для дальнейшего использования, способ передачи не регламентируется данным документом.

После этого необходимо просмотреть и при необходимости внести соответствующие изменения в классификаторы информации, содержание и (или) распространение которой противоречит законодательству Российской Федерации в части исполнения Федерального закона «Об информации, информационных технологиях и о защите информации». Данные классификаторы используются в подчиненных организациях как основа для формирования регламентов доступа к сети Интернет.

Кроме того, Администратор может разместить на сайте документацию, относящуюся к организации и внедрению СКФ, доступ, к которой он сочтет целесообразным для Администраторов нижестоящих организаций.

Ответственные лица в Муниципальных образовательных учреждениях, должны зарегистрировать на сервере СПП подотчетные им школы и определить учетные записи для их Администраторов, после чего передать регистрационные данные в соответствующие школы.

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).