ОРГАНИЗАЦИЯ БЕЗОПАСНОГО ДОСТУПА К СЕТИ ИНТЕРНЕТ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ (КОНТЕНТНАЯ ФИЛЬТРАЦИЯ).

Александр Геннадьевич Баданов,
badanov1@yandex.ru

Аннотация
В статье рассматриваются технологии и методики организации в образовательных учреждениях безопасного, защищённого доступа к сети Интернет.

Контентная фильтрация это интеллектуальный процесс анализа содержания тех или иных документов. В основном задачи фильтрации Интернет трафика решаются не с помощью интеллектуальных алгоритмов, а благодаря введению черных и белых списков разрешенных и запрещенных ресурсов. По утверждению специалистов в области информационной безопасности, на сегодня пока не решен вопрос анализа графических изображений для определения возможной опасности содержимого. Поэтому полностью автоматизировать процесс фильтрации (с требуемыми результатами) невозможен, если используется только одна технология анализа и фильтрации входящей информации.

Существующие технологии контентной фильтрации можно разделить на четыре группы:

- категоризация;
- списки ресурсов;
- контроль доступа;
- фильтрация данных.

Ни одна из обозначенных технологий не является универсальной — каждый подход имеет строго ограниченную область применения. Основная проблема - в качестве принимаемых решений, то есть правильностью выдаваемых на выходе результатов. Теоретически возможны ошибки двух типов: ошибки первого типа выдают «хороший» вердикт при «плохом» документе, а ошибки второго типа, напротив, выдают «плохой» вердикт при «хорошем» документе. Очевидно, что соотношение ошибок обоих типов существенно зависит от применяемых методов и технологий организации контентной фильтрации, а их критичность — от поставленной задачи.

Развитие современной науки, возможно, приведет к появлению новой и по-настоящему эффективной контентной фильтрации. Такая фильтрация уже не будет гадать о содержимом. Но сегодня с этой задачей способны справится только специалисты, однако в дальнейшем она окажется вполне посильной и для машин.

Для организации защищенного информационного пространства в образовательном учреждении придется многое сделать самостоятельно. Пакет программ «Первая помощь», в котором имелась программа для организации контентной фильтрации (работа которой правда вызывала множество нареканий), перестал использоваться в образовательных учреждениях. Каждый регион (каждая школа) должны самостоятельно организовать работу по исключению негативной, вредоносной информации на школьных компьютерах, подключенных к сети Интернет. Организация сетевой безопасности и контентной фильтрации потребует значительных временных затрат и принятия не простых управленческих решений. При этом наличие системы фильтрации не исключает необходимости обучения детей мерам безопасности и определенным правилам поведения в Интернете, но ограждает от часто навязываемого искаженного представления об окружающем мире.

Существует довольно много различных способов ограничить доступ учащихся к информационным ресурсам сети Интернет, содержимое которых несовместимо с целями образовательного процесса. Если использовать в комплексе несколько наиболее доступных способов, то это позволит обеспечить максимально возможную защиту от нежелательного Интернет-контента.

Условно разделим инструментарий, который можно использовать в различных операционных системах (Windows и Linux) (рассматриваются только бесплатные версии), на несколько категорий:

1. Специализированное программное обеспечение для контентной фильтрации
2. Функционал программ «Родительский контроль» или «Семейная безопасность»
3. Специализированные детские браузеры
4. Онлайн - сервисы для организации контентной фильтрации

Подробнее:

1. Использование специализированных программ для осуществления контентной фильтрации от нежелательного содержимого в сети Интернет:
    a. **Child Protect** http://cp.s-soft.org/ это социальный проект, цель которого оградить детей от нежелательного содержимого в Интернет. Работа программы незаметна для ребёнка. При попытке осуществить доступ на порносайт, который имеется в базе, браузер будет выдавать ошибку "Сервер не найден". У ребёнка будет создаваться ощущение, что такого сайта не существует. Также существует возможность опционально блокировать доступ к социальным сетям: ВКонтакте,

Одноклассники, МойМир@Mail.ru, FaceBook. Программа работает скрытно от диспетчера задач Windows.

b. **Программа K-9** http://www1.k9webprotection.com/ предназначена для эффективной защиты компьютеров на которых работают дети от аморального, запрещённого или травмирующего психику контента, рекомендуется как для защиты семейных компьютеров так и компьютеров работающих в учебных заведениях - школах, детских садах, институтах и т.д. Программа использует систему фильтрации содержимого сайтов по 55 категориям. Так же в программе имеются опции черного и белого списка. Можно дополнительно заблокировать любой сайт из разрешённой категории. Кроме всего прочего в настройках программы можно указать временной промежуток в течение которого пользователь будет иметь возможность пользоваться Интернетом. Так же имеется опция аудита активности пользователя, с возможностью просмотра списка заблокированных адресов. Программа имеет защиту от удаления.

c. **Naomi Internet Filter** фильтр Интернет- контента http://www.newestsoft.com/Windows/Web-Development/Wizards-Components/Naomi-3290.html. Эта программа предназначается для организации ограничения доступа к непристойным Интернет-ресурсам. Рекомендуется применять Naomi в учебных учреждениях. При своей работе утилита контролирует содержимое, загружаемое из интернета, и запрещает доступ к различным порно-сайтам, а также сайтам, содержащим насилие и пропаганду терроризма, азартные игры и т.д. Такая фильтрация осуществляется по ссылкам и ключевым словам (поддерживается 10 языков). Программа не нуждается в настройках, нужно только задать пароль, чтобы было невозможно отключить фильтрацию без ввода соответствующего пароля.

d. **Дополнение Adblocks Plus** к браузеру Mozilla FireFox. Это мультиплатформенное решение позволяет настроить контент -фильтрацию и дополнительно избавиться от надоедливой рекламы и всплывающих окон на сайтах. Для других браузеров также есть техническое решение этого дополнения http://adblockplus.org/en/installation . Список всех подписок доступен по ссылке http://adblockplus.org/en/subscriptions . Официальный сайт дополнения http://adblockplus.org/ru/

e. **NetPolice Lite** http://netpolice.ru/filters/lite/ – упрощенная версия платной программы NetPolice. К основным возможностям упрощённой версии относятся: регулярные информационные отчеты, 5 категорий фильтрации, доступ к настройкам по единому паролю, перенаправление на безопасный поисковик (http://search.netpolice.ru), возможность самостоятельного формирования списка сайтов для блокировки (до 5 URL), блокировка загрузки исполняемых файлов, предупреждение о переходе на небезопасные сайты и др.

f. **HandyCache** http://handycache.ru/ - это программа, которая экономит трафик, ускоряет загрузку страниц, блокирует рекламу и иное нежелательное содержимое и позволяет в автономном режиме (без подключения к Интернет) просмотреть любые посещенные ранее сайты. HandyCache – это кэширующий прокси-сервер. Он сокращает трафик до 3-4 раз за счет КЭШа. Любой из установленных на компьютере браузеров (и другие программы) могут использовать возможности программы, а значит, нет необходимости загружать одни и те же страницы несколько раз для просмотра в разных браузерах.

g. Программа **Kontrol Lite** http://www.kontrol.info/ Бесплатная версия Интернет-фильтра семейства Kontrol, которая позволяет блокировать порносайты. Отключить ее могут только родители,

знающие пароль. После загрузки и установки программы необходимо пройти регистрацию на сайте разработчика и получить login и пароль. Без них программа работать не будет.

h. **ParentalControl** http://www.securitylab.ru/software/270756.php – дополнение к браузеру Internet Explorer, которое помогает предотвратить доступ детей к сайтам для взрослых. Программа поставляется с набором настроенных фильтров, основанных на анализе сексуальных материалов, нецензурного языка, насилия и других критериев, позволяющим взрослым выбирать различные параметры фильтрации для своего ребенка. Также можно самостоятельно заблокировать или разрешить для просмотра любой сайт. Текущая версия работает только с этим браузером.

i. Межсетевой фильтр **Iptables** (Для операционных систем, серверов на базе **Linux**) обладает весьма широкими возможностями по настройке безопасности, что значительно усложняет его практическое освоение. Iptables позволяет: защитить ЛС от значительного количества удаленных атак, позволяет использовать прозрачное проксирование, скрыть локальную сеть за NAT— это усложнит злоумышленнику доступ к служебной информации.

j. Прокси-сервер **Squid** (Для операционных систем, серверов на базе **Linux**) является удобным инструментом для организации контентной фильтрации. При организации прозрачного проксирования, учащиеся не замечают, что нелегитимный контент отфильтровывается прокси-сервером. Squid позволяет: отфильтровывать Интернет-сайты, содержащие материалы не совместимые с задачами обучения и воспитания, вести журналы доступа ко всем посещенным сайтам, подсчитывать сетевой трафик. Кроме того, Squid кэширует прокси-сервер, то есть он сохраняет наиболее часто используемые файлы локально. Это

позволяет сократить Интернет-трафик и ускорить загрузку различных сайтов

2. Использование функции «родительского контроля» или «семейной безопасности» на компьютерах, с которыми работают школьники:
    a. Семейная безопасность **Windows Live 2011** для ОС Vista и 7 http://explore.live.com/windows-live-family-safety?os=winxp Для Windows XP – http://explore.live.com/windows-live-family-safety-xp Здесь можно выбирать, какое содержимое будет доступно детям в Интернете. Устанавливайте ограничения на поисковые запросы, отслеживайте посещаемые сайты, разрешайте или блокируйте доступ к ним. Фильтр Семейной безопасности должен быть установлен на каждом компьютере, который используют дети. Если фильтр не установлен, параметры безопасности не будут применены.
    b. Если в образовательном учреждении или на домашнем компьютере используются антивирусная программа **Kaspersky Internet Security версии 2010**, то в этой программе есть вкладка «Родительский контроль», где можно заблокировать доступ к нежелательным сайтам.
3. Использование специализированного браузера, созданного для детской аудитории:
    a. **Детский браузер Гогуль** http://www.gogul.tv/ специально разработанный для детей, их родителей и воспитателей. Эта программа мультиплатформенная, т.е. работает и в Linux и в среде Windows. Детский браузер Гогуль – обеспечит контроль посещения ребёнком сайтов в сети Интернете. Программа родительского контроля **Angry Duck** http://www.gogul.tv/about/#5 является так же бесплатным необязательным дополнением к детскому браузеру Гогуль, которая по желанию родителей может блокировать запуск всех

иных браузеров кроме Гогуля до ввода родительского пароля, а также выполнять другие функции по ограничению доступа детей к компьютеру.

4. Использование виртуальных социальных сервисов по осуществлению контентной фильтрации с ведением «белых списков» сайтов, посещение которых одобрено и специализированных поисковых машин в сети Интернет, которые специально организованы для работы с детьми:
    a. http://school.yandex.ru/ Это **проект школьный Яндекс**, который включает в себя фильтрацию контента. Можно использовать «по умолчанию» эту поисковую машину в школе.
    b. **NetPolice DNS** http://netpolice.ru/filters/dns-filter/ поможет Вам ограничить доступ к нежелательному содержимому, проводить мониторинг активности, снизить затраты на трафик Интернет. DNS-фильтр предоставляется всем желающим бесплатно. Для подключения фильтра необходимо выполнить несложную настройку на компьютере. После этого все запросы к Интернет-ресурсам будут автоматически проходить проверку на категорию запрашиваемого контента. Если запрашиваемый сайт будет относиться к нежелательной категории, то такой запрос будет заблокирован. Взамен заблокированного ресурса для просмотра будет предоставляться страница блокировки. DNS-фильтр – это дополнительная защита компьютера, так как интернет-ресурсы с нежелательным содержанием очень часто заражают компьютер вирусами, червями, шпионами и т.д. Таким образом, исключение доступа к небезопасным ресурсам значительно снижает риск нанесения ущерба компьютеру и данным, хранящимся на нем.
    c. **Портал «ТЫРНЕТ – Детский Интернет»** http://www.tirnet.ru Этот сервис включает в себя услугу «прокси», которая не позволит ребенку по баннерам и гиперссылкам перейти на

нежелательные ресурсы. Настроив особым образом свой браузер, Вы сможете установить на компьютере «белый список» сайтов в сети Интернет, адаптированных для детей. На сайтах из этого списка гарантированно не будет сцен насилия, кровавых иллюстраций к душераздирающим новостям и обнаженной натуры.

Это всего лишь небольшой обзор программ, решений и сервисов, которые можно использовать для организации безопасного информационного пространства в каждом образовательном учреждении.

Ниже приведен один из вариантов комплексной организации контентной фильтрации (все это настроено на каждом компьютере, за которым работают дети, есть варианты, когда основные сервисы настроены на сервере, и дополнены сервисами и программами на отдельных рабочих станциях):

- Использование программы контентной фильтрации на примере вкладки «Семейная безопасность» **Windows Live 2011** для ОС Vista и 7 http://explore.live.com/windows-live-family-safety?os=winxp
- Организация фильтрации с помощью систем поиска (например, в системе Яндекс в настройках блоков представления информации убираем все лишнее, а в настройках «Остальное»- «Настройка результатов поиска» включаем «Семейный фильтр» или используем поисковик «Школьный Яндекс» http://school.yandex.ru/
- Организации фильтрации с помощью дополнений (на примере браузера Mozilla Firefox- дополнение **Adblock Plus**

Имеет смысл познакомиться со всеми этими решениями, апробировать и помочь своим коллегам установить и настроить наиболее эффективные варианты. Их можно использовать как образовательном учреждении, так и на домашнем компьютере.

Литература

Основные федеральные законы об информационной безопасности:

- Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 3 января 2011(http://www.rg.ru/2010/12/31/deti-inform-dok.html);
- Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ О персональных данных (http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html);
- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации (http://www.rg.ru/2006/07/29/informacia-dok.html)
- Компонент «Родительский контроль», его основные возможности и его настройка в Kaspersky Internet Security http://www.intuit.ru/department/security/kasprot/3/
- Материалы сети Интернет (ссылки приведены в тексте)