Утверждаю
Начальник МУ «Управление образования
Надтеречного муниципального района ЧР»
_____И.С.Муцулханов
«___»_____2017г.

Рекомендации
по защите от доступа к информации, не совместимой с задачами образовательного учреждения.

1. Обзор систем, обеспечивающих контроль за содержанием потоков информации, передаваемых из учреждения образования в Интернет и получаемых из Интернета на компьютер (в локальную сеть) учреждения образования.
2. Рекомендации по защите школьников от просмотра и скачивания информациис веб-сайтов, не совместимых с задачами работы образовательного учреждения (порносайты, сайты антисоциальной направленности и т.п.).
3. Рекомендации по предотвращению неконтролируемого доступа и скачиванию из Интернета информации большого объема для внеучебных целей (видеофильмы, музыка, файловые архивы программного обеспечения и т.п.).

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.

Отметим, что 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

До сих пор мы говорили о том, что в учебном заведении есть проблема проникновения нежелательного контента внутрь учебной сети. Но существует также 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.

Масштабы ущерба от вредоносного контента

Прежде всего, следует сказать, что проблема защиты от вредоносного контента далеко не только школьная проблема. Использование Интернета сотрудниками или учащимися, не связанное с учебной или служебной деятельностью, получило название «киберслэкинг» (от англ. cyberslacking — дословно «кибербездельничание».

Учебные заведения отнюдь не первыми стали пытаться решить проблему фильтрации Интернета. Это, с одной стороны, говорит о том, что проблема глобальная и просто не решается, а с другой, что учебным заведениям в ряде случаев могут подойти решения созданные для организаций широкого профиля.

По данным компании IDC, свыше 40% обращений к Интернету с рабочего места никак не связано с профильным бизнесом, а согласно исследованиям компании WEBSENSE, из-за нецелевого использования Интернета сотрудниками во время работы американские организации теряют более 85 млрд. долл. — в виде упущенной выгоды от снижения производительности труда. Отметим также, что вирусы, трояны, шпионские программы и иные вредоносные коды тоже могут легко передаваться через Web.

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

В борьбе можно выделить организационные меры (назначение ответственных лиц, режим доступа в компьютерный класс, доведение до сведения учащихся норм поведения в Сети, ответственности за противоправные действия и т.н.) и технические. К техническим мерам относится фильтрация трафика, и 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.н.).

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.

Часто в школах установлено различное компьютерное оборудование и необходимы продукты фильтрации контента (Web и e-mail), работающие на различных платформах.

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 может 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.

Фильтры

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

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.