Рекомендации
для организации работы в образовательных учреждениях Кабардино-Балкарской Республики по ограничению доступа учащихся к информации, несовместимой с целями и задачами образования, в образовательных учреждениях

В рамках деятельности, направленной на защиту учащихся от информации, размещённой в Интернете и несовместимой с целями и задачами образования, в общеобразовательных учреждениях республики необходимо осуществлять постоянную, комплексную работу по контролю используемых Интернет-ресурсов, в том числе и с применением специализированного программного обеспечения (систем контентной фильтрации).

Для организации контроля доступа в ОУ к Интернет-контенту решающими являются следующие составляющие:

- нормативно-правовая база (создаётся и утверждается на региональном, муниципальном и школьном уровне);
- техническая (установленное и настроенное соответствующее программное обеспечение, контент-фильтры);
- педагогический контроль (доступ в Интернет осуществляется только в присутствии и под личным контролем педагогов).

Основной формой практического внедрения мероприятий по ограничению доступа учащихся образовательных учреждений к ресурсам Интернета, несовместимым с задачами образования, является принятие образовательными учреждениями следующих актов:

Правил использования сети Интернет,

Положения об ответственных лицах за функционирование средств контентной фильтрации доступа к сети Интернет в общеобразовательном учреждении,

Типовой инструкции для сотрудников образовательных учреждений о порядке действий при осуществлении контроля использования обучающимися сети Интернет,

Типовых правил использования сети Интернет в общеобразовательном учреждении.

Вышеперечисленные документы имеют статус локальных правовых актов и являются основой для внедрения соответствующих программно-технических средств.

При организации обеспечения ограничения доступа учащихся к Интернет-контенту, несовместимому с целями и задачами образования, необходимо обратить внимание на:

1. Наличие установленных программ фильтрации Интернет-контента на всех компьютерах, имеющих доступ к Интернету.

2. Обеспечение обновления программ фильтрации Интернет-контента и антивирусного программного обеспечения.

3. Проверку работы фильтрующих программ путем ввода контекстных слов.

4. Наличие ответственных по вопросам контроля доступа учащихся в Интернете.

5. Активизацию деятельности общественных советов ОУ по вопросам контроля доступа учащихся к ресурсам Интернета.

Необходимо помнить, что образовательный процесс включает множество различных областей, и фильтрация должна быть всеобъемлющей, настраиваемой, а также обеспечивать защиту от новейших угроз.

Варианты организации фильтрации и формы контроля доступа к Интернет-контенту в образовательных учреждениях

В большинстве образовательных учреждений КБР используются бесплатные ***программы контентной фильтрации*** «Net Police» и «Интернет Цензор».

Рекомендуется использовать сочетание разных методов, форм и вариантов контроля доступа к Интернет-контенту в ОУ.

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 («чёрные», «белые» списки, ключевые слова и т. п.).

«Белый список»: фильтрация реализуется по принципу «Запрещено всё, кроме того, что разрешено». Ответственный администратор сети/оператор по мере необходимости может добавлять «разрешённые» сайты в базу данных.

«Чёрный список»: требует построения и обновления базы, включающей запрещённый контент. В большинстве программ, фильтрующих Интернет-контент, имеется функция добавления информации в «чёрный список» вручную.

Фильтрация по «белому списку» рекомендуется для ПК учащихся, фильтрация по «чёрному списку» - для ПК учителей.

«Интернет Цензор» - бесплатная программа, с неограниченным сроком действия, устанавливающаяся также на персональный компьютер, которая кроме управления доступом к Интернет-ресурсам осуществляет также мониторинг использования ресурсов Интернета. Дистрибутив для скачивания, инструкции по работе с программой размещены на официальном сайте разработчика: http://www.icensor.ru. Имеется возможность обращения в техническую поддержку.

Основной функцией «Интернет Цензора» является блокирование доступа к интернет-сайтам, которые не входят в разрешенную «белую базу»

сайтов, составленную и предложенную компанией-разработчиком, а также в список, составленный самими пользователями. База сайтов, разрешённых компанией к посещению, постоянно обновляется. Обновления скачиваются программой с сервера компании автоматически раз в день.

«Белый список» в интерфейсе программы заполняют самостоятельно администраторы или учителя после скачивания и установки программы на персональный компьютер («родительский список»). Этот список для программы важнее, чем база компании-разработчика. При работе «Интернет Цензор» сначала обращается к «родительскому» списку разрешённых адресов. Кроме того, в программе имеется возможность создания «чёрного списка» ресурсов и запрещения посещения сайтов, доступ к которым разрешён компанией-разработчиком. Таким образом, запреты или разрешения администратора школьной сети будут приниматься во внимание в первую очередь.

При включении режима фильтрации вместо запрещенных к просмотру ресурсов браузер показывает страницу-заменитель. В случае если на разрешенном ресурсе есть нежелательные элементы, замене подвергается лишь часть страницы – та, что содержит части, не допущенные к просмотру.

Главный недостаток программы – недолговечность списков. Каждый день в Сети появляются сотни, а то и тысячи новых сайтов, поэтому включенные в программы списки быстро теряют свою актуальность, а значит, становятся неэффективными. Заявленные периоды обновления списков разработчиками соблюдаются не всегда, что может привести к открытому доступу к сайтам, содержащим информацию несовместимую с целями и задачами образования.

Информация о программе, дистрибутив бесплатной версии и информация о платных версиях *«Net Police»* размещена на вебсайте по адресу: http://netpolice.ru/filters .

Основные характеристики и порядок функционирования «Net Police»:

Основные особенности

- 5 категорий фильтрации
- Составление информационных отчетов
- Доступ к настройкам по единому паролю
- Перенаправление на безопасный поисковик (search.netpolice.ru)

Расширенная настройка

- Возможность самостоятельного формирования списка сайтов для блокировки (до 5 URL)
- Блокировка загрузки исполняемых файлов
- Предупреждение о переходе на небезопасные сайты

Дополнительные сервисы

- Возможность участия в оценке сайтов
- Подсветка ссылок на негативные ресурсы

Заявлено, что бесплатная версия программы ограничений в использовании фильтра не имеет, а используемая база ресурсов идентична базе в платной версии.

В программе «Net Police» используются две технологии фильтрации: URL-фильтрация и динамическая фильтрация.

URL-фильтрация позволяет точно определить тематику сайта. Перед тем, как открыть запрашиваемый ресурс, система проверяет, к какой категории он относится. Если данная категория заблокирована, то ученик не сможет открыть относящийся к ней сайт. Вместо него в браузере появится страница с предупреждением и безопасным поисковиком, так называемая "страница блокировки".

Для определения тематики Интернет-ресурсов, технология URL-фильтрации использует базу данных ЦАИР, которая в настоящее время считается самой полной базой русскоязычных сайтов (в ней содержится более 50 млн. классифицированных по категориям ресурсов). База данных ЦАИР используется в системе фильтрации, разработанной для всех школ РФ.

Второй технологией, используемой в фильтре «Net Police», является динамическая фильтрация. Этот инструмент анализирует текстовое содержимое Интернет-ресурсов. В поисковом запросе или на странице сайта слово, включённое в список запрещённых, будет заменено на "-----". Соответственно, поиск по запрещённым терминам будет невозможен. Кроме слов из категорий фильтрации (порнография, терроризм и др.) таким же способом блокируется и ненормативная лексика. Помимо того, что список блокируемых терминов регулярно обновляется, список слов для блокировки может быть дополнен на уровне образовательного учреждения.

Кроме того, в программе есть ряд инструментов для ограничения загрузки различных файлов (видео, музыка, архивы и др.).

Недостатками бесплатной версии программы относится слабая техническая реализация механизмов самозащиты от деинсталляции. Кроме того, бесплатная версия программа допускает пробои в фильтрации. Установка этого приложения, безусловно, уменьшает количество запрещенных сайтов, на которые может попасть учащиеся, но некоторые из подобных страниц остаются по-прежнему доступными.

Поэтому необходимо учитывать, что, даже используя обновления баз данных по нежелательным ресурсам, добиться 100%-ной фильтрации фактически невозможно.

К эффективным формам контроля доступа к Интернет-контенту в ОУ относится ***мониторинг активности пользователей.*** Мониторинг и протоколирование наглядно показывают «сёрфинг-профиль» пользователя. Учитель может проверить, где находился ученик, что просматривал, в какое время и как долго. Данные, как правило, защищены криптографически и хранятся в недоступном для неавторизованного просмотра виде. Любой посещенный ресурс может быть просмотрен, и впоследствии добавлен в список разрешённых или запрещённых листов.

Настоятельно рекомендуется ведение журнала учёта пользователей и времени начала и окончания их работы в кабинетах ОУ, имеющих ПК с выходом в Интернет.

Не рекомендуется отключать журнал контроля системы ПК в целях увеличения скорости его работы.

Контроль доступа как к информации в компьютере, так и к прикладным программам рекомендуется настроить таким образом, чтобы только авторизованные пользователи имели доступ к информации и приложениям, включая доступ в Интернет.

Не рекомендуется сохранять один и тот же пароль на длительное время.

Если сеть разведена по однопользовательскому принципу, требующему персональной аутентификации, рекомендуется попросить пользователей расписываться в отдельном журнале за получение паролей.

Установка и внедрение правил работы с паролями, ознакомление с этими правилами пользователей (как учащихся, так и учителей) помогут показать, что вопросы контроля доступа в Интернет в ОУ рассматриваются серьёзно.

Педагогический контроль

Для предотвращения случайного доступа к материалам, не соответствующим образовательным задачам, во время занятий контроль за использованием обучающимися сети Интернет должен осуществлять преподаватель, ведущий занятие. Преподаватель наблюдает за использованием компьютера и Интернета учащимися, принимает меры по пресечению попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.

Контроль доступа к Интернету и использования его ресурсов в образовательных учреждениях должен осуществляться как в учебное, так и во внеурочное время!

Во внеурочное время контроль должны осуществлять работники образовательного учреждения, специально определенные приказом руководителя ОУ. Они же принимают меры по пресечению попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования и сообщают классному руководителю о преднамеренных попытках обучающегося осуществить доступ к подобным ресурсам. Порядок назначения ответственных закрепляется в регламенте работы точки доступа к сети Интернет.

Правовая сторона вопроса и зоны ответственности.

В современных условиях продолжает формироваться правовое поле регулирования доступа учащихся к Интернет-ресурсам. Возникает много

вопросов о зонах ответственности и т. д. Рассмотрим несколько относящихся к теме правовых актов.

В соответствии с пунктом 4 статьи 29 Конституции Российской Федерации каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Ограничения права на свободное получение информации могут быть установлены только федеральным законом и только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (пункт 3 статьи 55 Конституции Российской Федерации).

В то же время, закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» является нормативным актом, предусматривающим отнесение информационной продукции к одной из категорий, попадающей под запрет распространения среди детей в зависимости от их возраста.

Предоставление безопасного доступа к печатным и электронным образовательным ресурсам, расположенным в открытом доступе и (или) в федеральных и региональных центрах информационно-образовательных ресурсов, является одним из федеральных требований к учебно-методическому обеспечению учебного процесса. При этом должно быть обеспечено ограничение доступа к информации, несовместимой с задачами духовно-нравственного развития и воспитания обучающихся и воспитанников (приказ Министерства образования и науки РФ от 04.10.2010 г. N 986 "Об утверждении федеральных требований к образовательным учреждениям в части минимальной оснащенности учебного процесса и оборудования учебных помещений").

В Федеральном законе от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», статье 14.1. о мерах по содействию физическому, интеллектуальному, психическому, духовному и нравственному развитию детей говорится:

«В целях содействия физическому, интеллектуальному, психическому, духовному и нравственному развитию детей и формированию у них навыков здорового образа жизни органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации, органы местного самоуправления ***в соответствии с их компетенцией создают благоприятные условия*** *для осуществления деятельности физкультурно-спортивных организаций, организаций культуры, организаций, образующих социальную инфраструктуру для детей (включая места для их доступа к сети "Интернет").*

Следует отметить, что фильтрация Интернет-контента в образовательных учреждениях является одной из мер по созданию таких условий.

Необходимо помнить, что образовательное учреждение несёт ответственность в случаях:

- если школа публикует информацию, несовместимую с задачами образования и воспитания, на своем сайте или в любых иных формах, включает её в учебные программы или во внеурочную деятельность. В данном случае ОУ попадёт в зону ответственности как распространитель;

- если сотрудники или ученики школы будут использовать в своих материалах информацию из Интернета с нарушением авторских и смежных прав, разглашать государственные или деловые тайны, они попадут в зону ответственности как распространители;

- если сотрудники школы не будут контролировать доступ учащихся в Интернет, это позволит считать их не выполняющими свои обязанности по обеспечению безопасности учащихся на территории школы.

Много вопросов возникает по применению актов законодательства антиэкстремистской направленности по отношению к образовательным учреждениям.

В соответствии со **ст. 4 Федерального закона от 25 июля 2002 г. N 114-ФЗ «О противодействии экстремистской деятельности»** субъектами противодействия экстремистской деятельности являются: федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления участвуют в противодействии экстремистской деятельности ***в пределах своей компетенции***.

Образовательное учреждение не несёт ответственности за случайный доступ к информации, несовместимой с целями и задачами образования, размещенной не на Интернет-ресурсах образовательного учреждения. Школа является потребителем услуги доступа к ресурсам Интернета для реализации своей основной уставной деятельности - обучения.

В то же время, необходимо помнить, что существует возможность случайного обнаружения обучающимися ресурсов, содержание которых несовместимо с целями и задачами образовательного процесса.

Руководители общеобразовательных учреждений должны обеспечить организацию работы по рассматриваемым вопросам, учитывая, что возможность доступа учащихся со школьных компьютеров к информации, несовместимой с образовательным процессом, должна блокироваться не только техническими средствами, но и правильной организацией работы персонала, систематическим контролем со стороны ответственных лиц и педагогических работников учебного заведения, а также целенаправленно проводимой работой по обучению учащихся правильно пользоваться Интернетом.

Приложение

Методика оценки качества фильтрации предложена в методических рекомендациях Министерства образования и науки РФ, Федерального агентства по образованию РФ и НФПК «Регламентирование порядка внесения изменений в список категоризированных ресурсов сети Интернет». В частности, **в п. 5.1** говорится:

«Проверка производится посредством проверочных слов «секс, порно, проститутки». Открывается сайт http://www.yandex.ru, в строке поиска вводится проверочное слово, затем просматриваются ссылки на первых пяти страницах с результатами поиска, выданных поисковой системой. Если при открытии страницы по ссылке отображается строка «403 Forbidden» - значит, срабатывает контентная фильтрация, иначе данный сайт не блокируются».

Сводный процент открытия нежелательных сайтов по всем проверочным словам определяет качество фильтрации:

1) от 30% и более - код оценки - 6 - фильтрация выполняется, но используется не актуальное информационное обеспечение;

2) от 10% до 30% - код оценки - 7 - фильтрация выполняется удовлетворительно, но следует обратить внимание на актуализацию ИО;

3) менее 10% - код оценки - 8 - фильтрация выполняется с высоким качеством.

Полностью с методикой оценки качества фильтрации Интернет-контента можно ознакомиться на вебсайте по адресу: http://www.ed.gov.ru/td/srfcp/pnpo/rtosinfot/metinf/mm/).

Полезные ссылки

Федеральный список экстремистских материалов на официальном сайте министерства юстиции РФ: http://www.minjust.ru/nko/fedspisok

Центр безопасного Интернета в России (представлены советы и рекомендации для родителей и детей всех возрастов): http://www.saferunet.ru

«Горячая линия «Сообщи о противоправном контенте»: http://www.saferunet.ru/hotline/content.php

Сайт «Линия помощи «Дети России Онлайн»: http://www.detionline.com/

Справочник Google по детской безопасности в Интернете: http://www.google.ru/goodtoknow/familysafety/

Сайт «Фонд Развития Интернет»: http://www.fid.ru/

Бесплатный российский Интернет-фильтр для детей «ИНТЕРНЕТ ЦЕНЗОР» http://www.icensor.ru/

Сайт и контент-фильтры NetPolice: http://www.netpolice.ru/

Сайт (на англ. яз.) и контент-фильтр DansGuardian под LINUX (бесплатен для некоммерческого использования): http://dansguardian.org/?page=download2
Инструкции по установке и настройке DansGuardian на русск. яз.: http://pclinuxos.su/index.php/server/nat-proxy-server/142-dansguardian-luchshaya-filtratsiya-kontenta

Сайт SQUID (на англ. яз.) - программный пакет, реализующий функцию кэширующего прокси-сервера для протоколов HTTP, FTP, Gopher и (в случае соответствующих настроек) HTTPS: http://www.squid-cache.org/