Печать

Памятка по ограничению доступа информации, распространяющейся в сети Интернет, способной причинить вред здоровью и развитию детей.

14 Марта 2016

Контент – фильтрация.

Каждый пользователь при работе в Интернете сталкивается с нежелательным контентом. Речь идет не только о той информации, которую пользователь не хотел получать. Нежелательным контентом являются:

- вирусы, трояны и прочие вредоносные объекты;

- фишинг, перехват паролей;

- сетевые атаки;

- утечка важной информации;

- киберпреследование и злоупотребление персональными данными.

Кроме того, существует определенная информация, доступ к которой необходимо ограничить, например, если за компьютером находится ребенок.

Решением всех этих проблем является использование системы контетной фильтрации. Похожей системой пользуются антивирусы и фаерволлы, защищающие компьютер от вирусов и сетевых атак.

Принципы контентной фильтрации

Фильтрация контента может осуществляться по принципу «запрещено все, кроме того, что разрешено» или «разрешено все, кроме того, что запрещено».

Конечно, построить фильтрацию по принципу «запрещено все, кроме того, что разрешено» довольно просто. Возможно, она подойдет для защиты от нежелательного контента младших школьников, но в этом случае многие возможности Интернета становятся недоступны.

Элементарная фильтрация может быть основана на применении локальной программы. Например, можно запретить в браузере доступ к определенным сайтам, однако перечислить все нежелательные сайты невозможно. Для этого требуется огромная база данных, которая должна постоянно обновляться. Для полноценной реализации данного вида фильтрации необходимо проиндексировать миллиарды web-страниц, а это под силу только крупным провайдерам.

Варианты фильтрации контента

Контент может фильтроваться на трех уровнях: провайдера, шлюза в Интернет защищаемой сети и клиентской станции, а также в Сети на уровне онлайновых сообществ. Например, форумы и чаты часто имеют модераторов, которые могут редактировать или удалять материал, нарушающий законы государства и правила того или иного сообщества. Однако большинство USENET-групп являются немодерируемыми.

В Сети существуют различные сервисы, предоставляющие безопасный учебный контент.

Многие пользователи хотят оградить членов своей семьи, особенно несовершеннолетних детей, от интернет-ресурсов «для взрослых», поэтому многие поисковые системы предлагают Safe Search (безопасный поиск). В поисковой системе Яндекс подобная функция называется «семейный поиск».

Делая запрос в «семейном» Яндексе, вы не наткнетесь на ресурсы с нецензурной лексикой и порнографией, то есть не встретите ничего, что запрещено «детям до 16». Есть два способа поиска с помощью «семейного» Яндекса.

Во-первых, можно сделать запрос не на **www.yandex.ru**, а на **http://family.yandex.ru**. Во-вторых, можно настроить браузер так, что даже при работе с обычным Яндексом «взрослые» ресурсы будут отфильтрованы.

Страницы и сайты фильтруются полуавтоматически: из результатов поиска исключаются «взрослые» сайты, а также все страницы, содержащие «нехорошие» слова.

Функция «безопасного поиска» реализована в таких популярных поисковых машинах, как Google, Yahoo!, Dogpile, AltaVista, Lycos, AllTheWeb и MSN.

Способы фильтрации контента

Отслеживать и блокировать нежелательную часть контента возможно следующими способами:

1. Фильтрация сайтов осуществляется с помощью любого браузера или Интернет-фильтра. Они контролируют поток Интернет-трафика через определение категории сайта по его содержимому. Это особенно актуально для ресурсов, которые содержат информацию разных категорий. Дело осложняется тем, что технологии не стоят на месте. Сайты создаются с помощью новых инструментов, а это требует разработки новых технологий фильтрации Интернет-трафика.
2. **Выбор особого тарифа у провайдера.**

Практически все провайдеры, например, РосТелеком или Мегафон за дополнительную плату предоставляют такую возможность.

плюсы:

Невозможность обхода фильтров путём изменения ПО компьютера (то есть бесполезно добавлять учетные записи или переустанавливать систему);

не требуется знаний компьютера (они сами всё подключат без вашего участия);

гарантия качества (провайдер несёт ответственность за качественную фильтрацию контента)

минусы:

низкая скорость (зависит от метода фильтрации, используемого провайдером);

попадание под фильтры «безвредных» сайтов (фильтрация часто работает по ключевым словам, содержащимся в тексте, поэтому блокируются некоторые весьма нужные сайты, некоторые страницы новостных порталов, фотогалереи сайтов, гостевые книги а также (по непонятным причинам) и некоторые другие);

невозможность временно отключить фильтр (бывают моменты, когда дети уже давно уснули и хочется посмотреть кино для взрослых, а вот НЕТ – не получится)

2. Антивирус, оснащённый семейным фильтром.

Антивирус в условиях жёсткой конкуренции становится уже больше чем просто антивирусом. Он оснащается всевозможными экранами, дополнительными возможностями и способностями. К одной из таких возможностей можно отнести Семейный фильтр

плюсы:

такая фильтрация убережёт вас не только от сайтов с сомнительным содержанием, но также от вредоносного кода;

возможность настройки фильтра;

рейтинг сайтов (при использовании дополнительных плагинов)

минусы:

Использование только с оплаченной лицензией антивируса (в бесплатных антивирусах такой возможности нет);

Слабый контроль (как правило, такие фильтры не обеспечивают стопроцентной защиты от нежелательного контента);

3. Использование прокси-сервера с чёрным или белым списком.

Этот вариант годится в первую очередь для локальной сети, где весь трафик идет через головной компьютер или сервер.

плюсы:

полный контроль сразу нескольких компьютеров;

возможность управления черными или белыми списками *(Черный запрещает только посещение тех сайтов, которые в нём присутствуют, белый список разрешает посещение только указанных сайтов)*;

статистика (полный отчёт о посещённых сайтах и сайтах, посещение которых было предотвращено);

возможность временного отключения фильтров для всех или отдельных участников сети

минусы:

Сеть должна иметь соответствующую архитектуру

Зависимость от головного компьютера (сервера)

Необходимость вручную составлять черный или белый списки (или искать в интернете уже составленные правила и дорабатывать их)

4. Использование специального ПО.

Эти программы устанавливаются отдельно и служат конкретно для фильтрации просматриваемого контента. С каждым днём выбор этой продукции всё увеличивается, производители расхваливают свои продукты, оснащают их всевозможными дополнительными модулями и стремительно завоёвывают своё «место под солнцем» пользуясь тем, что отечественный интернет не имеет цензуры.

Что касается программного обеспечения, которое помогает осуществлять контентную фильтрацию, то их существует очень много. Они представлены в виде комплексных контент-фильтров и маленьких плагинов для Интернет-браузеров. Особенно богат выбор среди средств защиты детей от Интернет-угроз. С помощью современного ПО можно ограничить чаду доступ в Интернет, блокировать взрослый контент, следить на какие страницы он заходит и сколько времени проводит в Сети.

С помощью стандартного контент-фильтра можно:

- регулировать время прибывания в Интернете;

- регулировать доступ на определенные сайты;

- запрещать посещение сайтов с определенным контентом;

- отключить загрузку флеш-рекламы;

- отключить всплывающие окна;

- запрещать автоматические переходы на другие сайты.

Существует несколько фильтров с функцией родительского контроля, поддерживающих русский язык. Это NetPolice, K9 Web Protection, KidGid и ContentKeeper.

Технологии не стоят не месте, они постоянно развиваются, пополняя Интернет новыми возможностями и новыми угрозами. Поэтому крайне важно вовремя скачивать обновленное защитное программное обеспечение, чтобы защитить себя и своих близких от Интернет-угроз.

Автоматизированная информационная система "Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в России запрещено"

Нормативным актом, где подробно перечислена информация, распространение которой запрещено, является Федеральный закон от 29 декабря 2010 г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

В частности, в этом законе к ней относится информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;
- отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям или другим членам семьи;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера;
- о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

С целью ограничения доступа к сайтам в Интернете, содержащим такую информацию, была создана автоматизированная информационная система "Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в России запрещено".

Кроме того, в соответствии с пунктом 6 Правил создания, формирования и ведения единой автоматизированной информационной системы «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено», в электронном виде создана форма для приема обращений органов государственной власти и органов местного самоуправления, юридических лиц, индивидуальных предпринимателей, общественных объединений и иных некоммерческих организаций, а также граждан о наличии на страницах сайтов в сети «Интернет» запрещенной информации и для взаимодействия с указанными органами власти, физическими и юридическими лицами в рамках деятельности по формированию и ведению единого реестра. Эта форма размещается по адресу:
http://eais.rkn.gov.ru/.

В случае признания информации запрещенной к распространению, доступ к ней ограничивается в установленном порядке.

Реестр ведется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Информацию о внесении конкретных интернет-ресурсов в реестр можно узнать на официальном сайте Роскомнадзора.

Адрес данной страницы в интернете: https://46.xn--b1aew.xn--p1ai/news/item/8054345