**Организация контент-фильтрации в школе с контролируемым доступом в сеть Интернет**

Рассмотрим основные угрозы, которые могут встретиться в интернете. Это:

«Взрослые» сайты

Фишинговые сайты

Пиратский софт

Сайты, распространяющие вирусы

Сайты экстремистской направленности

Ресурсы с неконтролируемым содержимым

Социальные сети

Файлообменники

Фото/видео хостинги

Блоги, форумы, чаты

Онлайн-игры

Многие из этих угроз не нуждаются в комментариях, однако, понятие фишинговых сайтов я бы пояснил. Итак, фишинговый сайт – это поддельный сайт какой-либо организации, который выглядит точно так же как и оригинал, но создан он с целью получения идентификационных данных пользователя (e-mail, логин, пароль…). Эти данные могут быть использованы для похищения денежных средств с ваших счетов, рассылки спама от вашего имени и т.д. Рассмотрим основные проблемы, с которыми сталкивается большинство систем контентной фильтрации. К ним можно отнести следующие:

* На одном сайте может располагаться и «плохой», и «хороший» контент
* Постоянно создаются новые сайты, которые попадают в базу только по истечении некоторого времени
* Сложно проверять зашифрованный траффик
* Сложно блокировать соединения пиринговых сетей (p2p)
* Часто «хорошие» сайты живут за счёт рекламы «плохих»



В нашей школе применяется комплексный подход для организации контент - фильтрации интернет траффика, установлено сразу несколько решений: фильтрация с помощью настроек безопасности браузера, фильтрация с помощью антивирусных программ, Zentyal, DansGuardian, Squid. Всё это в сочетании с контент - фильтром интернет провайдера обеспечивает высокий уровень фильтрации нежелательного контента. Перейдём к рассмотрению конкретных решений, позволяющих организовать фильтрацию контента в школе:

1. организация разграничения прав доступа к ресурсам сети Интернет для различных групп пользователей локальной сети образовательного учреждения;
2. фильтрация трафика на основе «черных» и «белых» списков;
3. ведение электронного журнала работы пользователей в сети Интернет, доступного через вебинтерфейс, создаваемого автоматически на основе отчета о работе прокси-сервера.

"Белые списки" - подразумевают перечень ресурсов, доступ к которым разрешен.

Несомненно, что "Белые списки" для образовательного учреждения должны содержать только те ресурсы, которые отвечают образовательным задачам школы.

"Черные списки" - подразумевают перечень ресурсов доступ, к которым запрещен.

Программа для фильтрации трафика: DansGuardian. Эта программа способна обеспечить различный уровень доступа пользователей, фильтрацию контента, а также позволяет организовать фильтрацию на основе "черных" и "белых списков", запросов. Используется совместно с прокси-сервером Squid и обеспечивает фильтрацию по содержимому.

Zentyal — это пакет серверного программного обеспечения с открытым исходным кодом. Он может выступать в роли сетевого шлюза, единого центра безопасности сети. Защищает компьютерную сеть от внешних атак, вторжений и внутренних угроз безопасности. Управление всеми аспектами работы дистрибутива производится через web-интерфейс, в рамках которого объединено около 40 различных модулей для управления сетью, сетевыми сервисами, офисным сервером и компонентами инфраструктуры предприятия. Поддерживается быстрая организация работы шлюза, межсетевого экрана, почтового сервера, VoIP (Asterisk), VPN-сервера, прокси (squid), файлового сервера, системы для организации взаимодействия сотрудников, системы мониторинга, сервера для резервного копирования, системы обеспечения сетевой безопасности, и т.п. Настройка всех модулей осуществляется через систему мастеров и не требует ручной правки файлов конфигурации. В Zentyal удобно организованно:

|  |  |
| --- | --- |
| Панель администрирования. Удобно, красиво, ничего не раздражает. Слева меню | |
| модулей, по центру виджеты |  |

1)

1. Создание групп пользователей с различными правами доступа к сети интернет
2. Правила фильтрации позволяют быстро добавить нужный сайт в «белый список»
3. Грамотный перевод на русский язык

