

Требования к настройке Профилей.

1. Установка контентной фильтрации.

В зависимости от схемы организации локальной сети у Абонента и схемы подключения оборудования Абонента к интернет существуют разные варианты подключения их к сервису контент-фильтрации:

Если есть центральный сервер или маршрутизатор/роутер

Если у Абонента, есть центральный сервер или маршрутизатор/роутер (ADSL, Wi-Fi), через который выходят в интернет все прочие компьютеры, то наиболее оптимальным вариантом настройки будет настройка подключения к фильтру непосредственно на самом сервере, маршрутизаторе/роутере.

Порядок настройки подключения в этом случае следующий:

1. В случае статичного (неизменного) внешнего IP адреса Абонента, достаточно на сервере или маршрутизаторе указать в настройках DNS для сетевого соединения адрес – 193.58.251.251.
2. В настройках всех сетевых соединений (как интернет, так и локального) на сервере/маршрутизаторе НЕ должны быть указаны другие DNS серверы. Также поле DNS для IPv6 должно быть пустым и отключено автоматическое получение DNS. В противном случае фильтрация не будет работать.
3. При использовании прокси (обычного или прозрачного), необходимо указывать DNS сервер в настройках прокси сервера или отключить проксирование. В противном случае фильтрация работать не будет.
4. После прописывания DNS в своей системе привяжите ваш внешний IP адрес в личном кабинете в разделе «Настройки — Сети — Статические IP-адреса» (по умолчанию, IP-адрес автоматически прописывается в личном кабинете).

Настройка статических IP-адресов.

Вы можете добавить еще 9 адресов

IP адрес	Профиль	
46.146.226.114	Тестовый	Основной

Стенд

5. После этого можно переходить к настройке правил фильтрации.

Все компьютеры подключены к интернет напрямую или через маршрутизатор провайдера (одноранговая сеть)

1. В этом случае единственным вариантом будет настройка контентного фильтра
2. непосредственно на каждом компьютере Абонента:
3. На компьютерах под управлением ОС Linux производится настройка DNS аналогично описанному в предыдущем разделе (центральный сервер).
4. Чтобы ученики не могли отключить фильтр они должны работать под учетными записями с ограниченными правами.
5. Держите пароль от вашего личного кабинета в тайне, чтобы никто не мог с его помощью отключить фильтрацию.
6. После этого можно переходить к настройке правил фильтрации.

Рекомендуемые правила контентной фильтрации и безопасный поиск

В штатном режиме, возможна работа с ограничением по категориям интернет-ресурсов. Список категорий определяется методическими рекомендациями Министерства образования и науки по блокировке не соответствующих задачам образования ресурсов интернет в образовательных организациях.

Мы настоятельно рекомендуем включить фильтрацию следующих категорий (раздел Фильтр в личном кабинете):

- Федеральный список Минюста (в эту категорию входят только явно указанные в федеральном списке сайты, за исключением таких сайтов как vk.com, youtube.com)
- Агрессия, расизм, терроризм
- Грубость, матерщина, непристойность
- Запаркованные домены
- Наркотики
- Реклама и баннеры
- Плагиат и рефераты
- Прокси и анонимайзеры
- Ботнеты
- Сайты, распространяющие вирусы
- Фишинг
- Алкоголь и табак
- Знакомства
- Казино, лотереи, тотализаторы
- Оккультизм и астрология
- Порнография и секс
- Сайты для взрослых
- Радио и музыка онлайн
- Торренты и P2P-сети
- Файловые архивы
- Фотогалереи
- Фильмы и видео онлайн
- Досуг и развлечения
- Компьютерные игры
- Социальные сети
- Новости и СМИ
- Форумы
- Чаты и мессенджеры

Чтобы включить рекомендованные настройки блокировки по категориям в разделе Фильтр личного кабинета нажмите в меню левой колонки кнопку «Для школ» и нажмите кнопку Сохранить.

Включите опцию «Блокировать неизвестные сайты» (в особых настройках на странице Фильтр), чтобы блокировать все сайты неизвестные для сервиса и не попасть на только что появившийся сайт с неподходящим контентом.

Включите опцию «Использовать безопасный поиск». Выдача этого поиска фильтруется от запрещенной информации (экстремистские материалы, порнография, наркотики, нецензурная речь, фишинговые и вирусные сайты).

В категорию «Федеральный список Минюста» входят только явно указанные в федеральном списке экстремистских материалов сайты. Существующая технология фильтрации не позволяет заблокировать абсолютно все сайты, содержащие произвольно выбранный тестовый, графический, аудио или видео материал из федерального списка экстремистских материалов, указанные без адреса их размещения в интернет. В связи с этим для более надежной защиты от экстремистских материалов можно использовать режим работы «Только по белому списку» и предоставлять доступ только к тем интернет-ресурсам, которые ваше учебное заведение определяет самостоятельно.

При использовании исходной поисковой системой шифрованного протокола HTTPS, перенаправление будет работать некорректно. Поэтому необходимо в свойствах браузера поменять поисковую систему по умолчанию на ту которая работает по протоколу HTTP или отключить использование шифрованного протокола.

Работа только по белому списку

Как было написано выше, существующая технология не позволяет ограничить доступ к определенным видам запрещенной информации со 100% гарантией. В связи с этим для максимально возможной защиты рекомендуется использование режима «Работа только по белому списку».

В данном режиме доступ предоставляется только сайтам явно включенным вами в белый список (разрешенные ресурсы), а также сайтам входящим в различные каталоги образовательных ресурсов (например <http://window.edu.ru>) Добавление ресурсов в белый список производится на странице «Домены» в личном кабинете. Включение режима работы только по белому списку производится на странице «Фильтр» (под списком категорий). Поставьте галочку у опции и нажмите кнопку «Сохранить». Применение настроек занимает от 2 до 3 минут со стороны наших серверов. Если вам необходимо добавить большой список ресурсов в белый список, то вы можете прислать его нам в техническую поддержку для проверки и мы его добавим в глобальный белый список, чтобы сделать доступным для всех учебных заведений.

Настройки браузеров, установка поиска по умолчанию

Часто проверяющие смотрят журналы браузеров на наличие в них посещенных ранее запрещенных сайтов, поэтому рекомендуется принудительно выключать в браузерах ведение журнала и истории, либо включать настройку очистки истории при выходе из браузера. Кроме этого вы должны установить безопасный поиск как поиск по умолчанию, удалив все прочие поисковые системы из браузера или отключив их.

Firefox

1. Зайдите на страницу безопасного поиска poisk.skydns.ru
2. Щелкните на маленький треугольник возле названия текущей выбранной поисковой системы.
3. Выберите пункт «Добавить «Безопасный поиск»».
4. Еще раз нажмите на треугольник для вызова списка поисковых систем и выберите пункт «Управление поисковыми системами».
5. Выберите все прочие поисковые системы и нажмите «Удалить», чтобы «Безопасный поиск» остался единственным элементом в списке.

Chrome

1. Зайдите на страницу безопасного поиска poisk.skydns.ru
2. Щелкните правой клавишей мыши по строке с именем сайта и выберите из списка «Изменить поисковые системы».
3. Наведите мышью на строку «Безопасный поиск» и нажмите на «Использовать по умолчанию».
4. Удалите все прочие поисковые системы. Крестик для удаления появляется справа при наведении мыши на строку с названием поисковой системы.

Internet Explorer

1. Зайдите на страницу безопасного поиска poisk.skydns.ru
2. Щелкните на треугольник рядом с кнопкой с лупой.
3. Выберите пункт «Добавление поставщика поиска» и далее «Безопасный поиск».
4. В открывшемся диалоге поставьте галочку «Сделать поставщиком поиска по умолчанию» и нажмите «Добавить».
5. Снова нажмите на треугольник рядом с кнопкой с лупой и выберите пункт «Управление поставщиками поиска».
6. В открывшемся окне надстроек удалите все прочие поисковые системы.

Организационные меры

Не забывайте, что контентная фильтрация - это не только установка фильтра, но и ряд организационных мероприятий.

Согласно требованиям Министерства образования и науки РФ, каждое учебное заведение должно иметь регламент, определяющий порядок доступа в интернет и ответственных за контентную фильтрацию.

Образец регламента и прочих документов можно посмотреть в приложениях.

Удостоверьтесь, что в вашем регламенте четко обозначены:

- ответственные за фильтрацию,
- порядок допуска учеников и третьих лиц к компьютерам для использования интернет,
- обеспечение доступа только к безопасной поисковой системе и запрет на использование других систем,
- порядок действий при обнаружении доступа к сайтам с запрещенной информацией.

Также всегда имейте под рукой актуальную копию федерального списка экстремистских материалов (<http://minjust.ru/extremist-materials>) в электронном или печатном виде.

Если в вашем регионе приняты локальные нормативные акты/законы по порядку доступа учебных заведений в интернет и/или контентной фильтрации, то также подготовьте и имейте их печатные копии.