Администрация Томской области

Областное государственное автономное учреждение культуры

«Томская областная универсальная научная библиотека им. А.С. Пушкина»

Фильтрация доступа к Интернет-ресурсам

РЕКОМЕНДАЦИИ

Томск 2014

ББК 32.973.202

Ф 57

Составитель: Перебоев О.Н.

Редактор: Чередникова Л.В.

Фильтрация доступа к Интернет-ресурсам / Обл. гос. автономное учреждение культуры «Томская обл. универс. науч. б-ка им. А.С. Пушкина»; сост. О.Н. Перебоев. – Томск, 2014. – 13 с.

Рекомендации по фильтрации доступа к Интернет-ресурсам.

Вторая половина XX и начало XXI века ознаменовались очередным этапом научно-технической революции – внедрением во все сферы жизни информационно-коммуникационных технологий и развитием глобальной компьютерной сети – Интернета. Они составляют фундамент и материальную базу для перехода к информационному обществу, к новой ступени в развитии современной цивилизации.

Рост количества и объема ресурсов сети Интернет обусловливает необходимость поиска новых эффективных методов решения задачи ограничения доступа к ресурсам нежелательной тематики и содержания.

Рассмотрим задачу ограничения доступа рабочей станции к нежелательным ресурсам в сети Интернет. Необходимо обратить внимание на важные моменты:

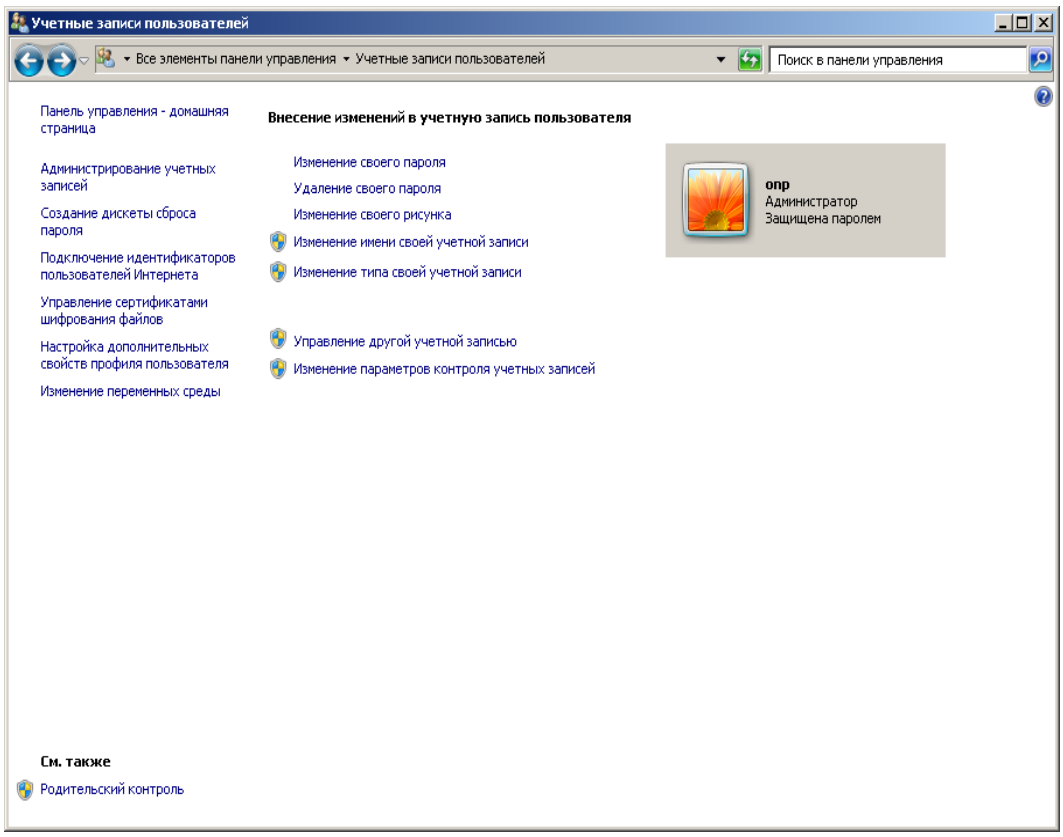
- Рассматривается защита отдельного компьютера, но не сети организации в целом.
- Доступ к спискам Роскомнадзора есть только у операторов связи, поэтому ограничить в полной мере доступ может только провайдер. Фильтрация по этим спискам рассматриваться не будет.

Подготовка компьютера

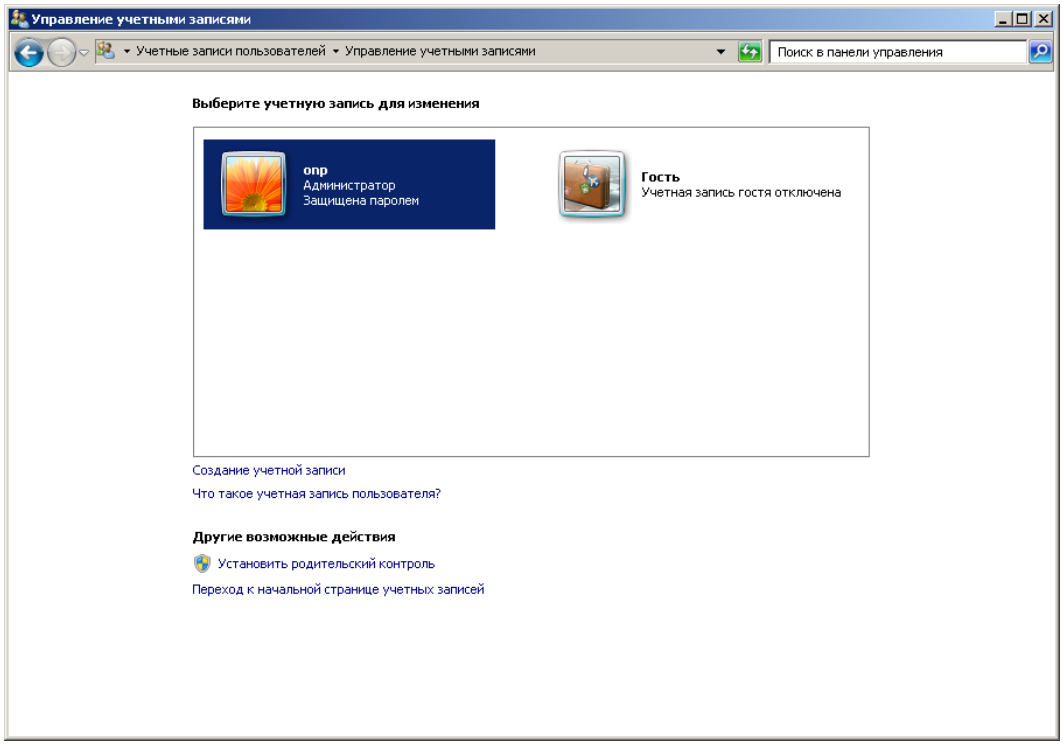
Первый шаг в фильтрации доступа – это разделение парка компьютеров на зоны доступа: детскую и взрослую. Если такой возможности нет, можно сделать разные учетные записи для детей и для взрослых. Учетные записи пользователей не должны иметь права Администратора. Независимо от назначения компьютера, учетная запись с правами Администратора должна иметь пароль.

Учетные записи создаются следующим образом:

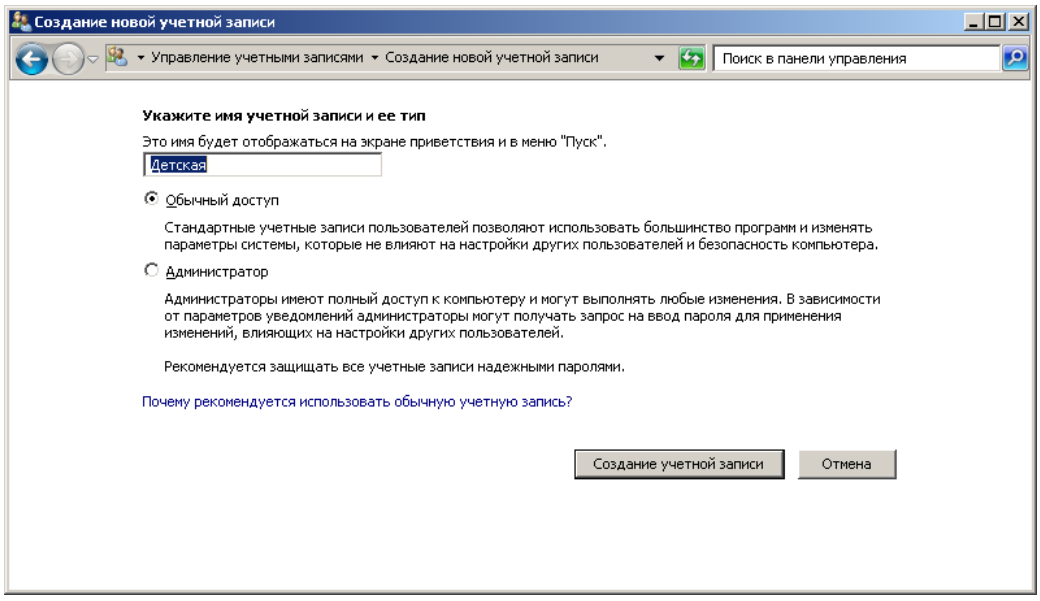
1. Открываем панель управления.



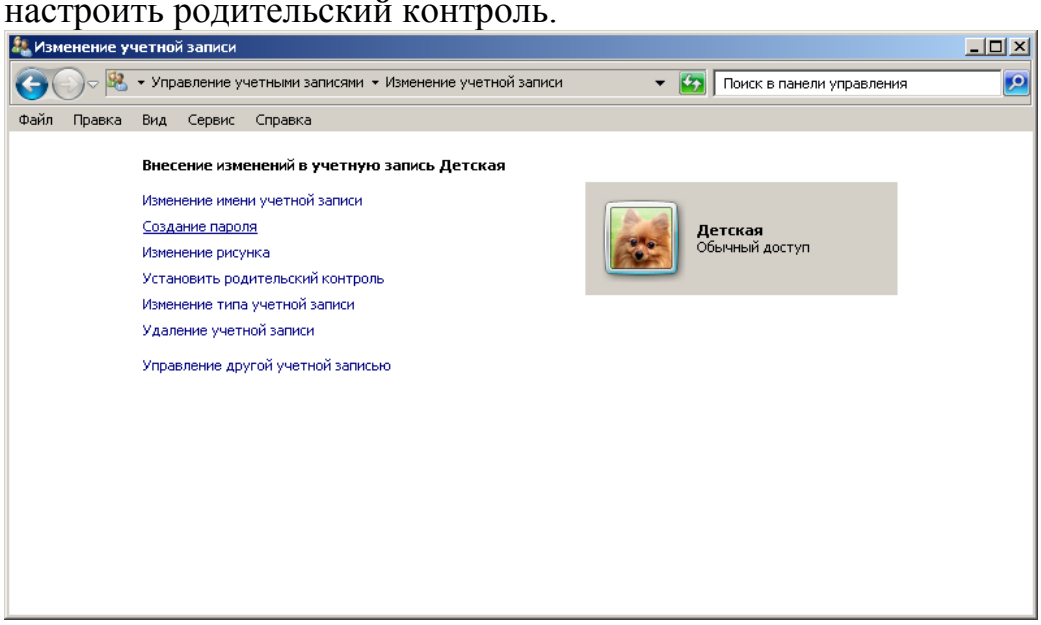
2. Запускаем программу «Учетные записи пользователей».
3. Нажимаем «Управление другой учетной записью».
4. Выбираем «Создание учетной записи».



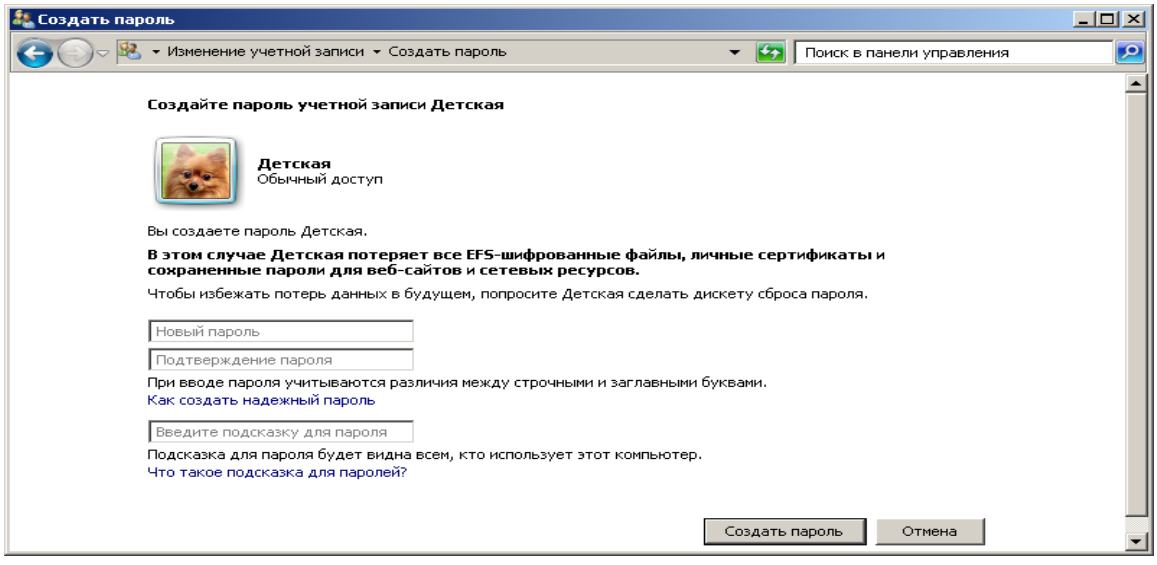
5. Указываем имя пользователя и тип учетной записи. Нажимаем на кнопку «Создание учетной записи».



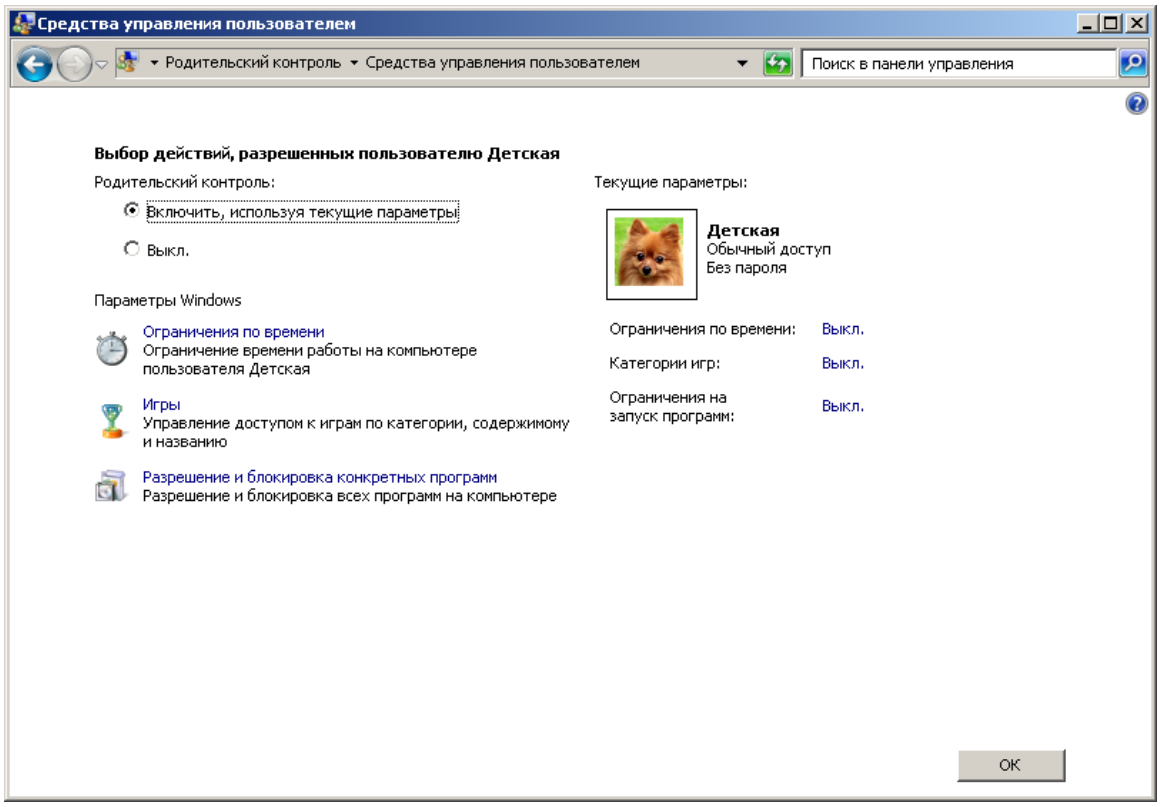
6. Далее из списка учетных записей, выбираем созданную запись. Откроется окно учетной записи, в котором можно создать пароль и настроить родительский контроль.



7. Задаем пароль.



8. Если создаем учетную запись для ребенка, можно настроить функцию «Родительского контроля», которая ограничит время сеанса работы, запуск программ и игр.



Способы фильтрации доступа к ресурсам

Фильтрация доступа к ресурсам – блокирование попытки получить доступ к информационному ресурсу целиком либо частично. Основана на анализе адреса ресурса. Анализ содержания ресурса является ресурсоемкой задачей, зато позволяет закрывать доступ к отдельным фрагментам, графическим элементам, при этом не блокируя доступ к ресурсу.

Фильтрация ведется с помощью 2-х политик:

- Черный список – доступ разрешен на любой сайт, кроме ресурсов из списка.
- Белый список – доступ разрешен на сайты из списка, остальные информационные ресурсы закрыты.

Фильтрация средствами компьютера

Рассмотрим способы фильтрации доступа на каждом отдельном компьютере.

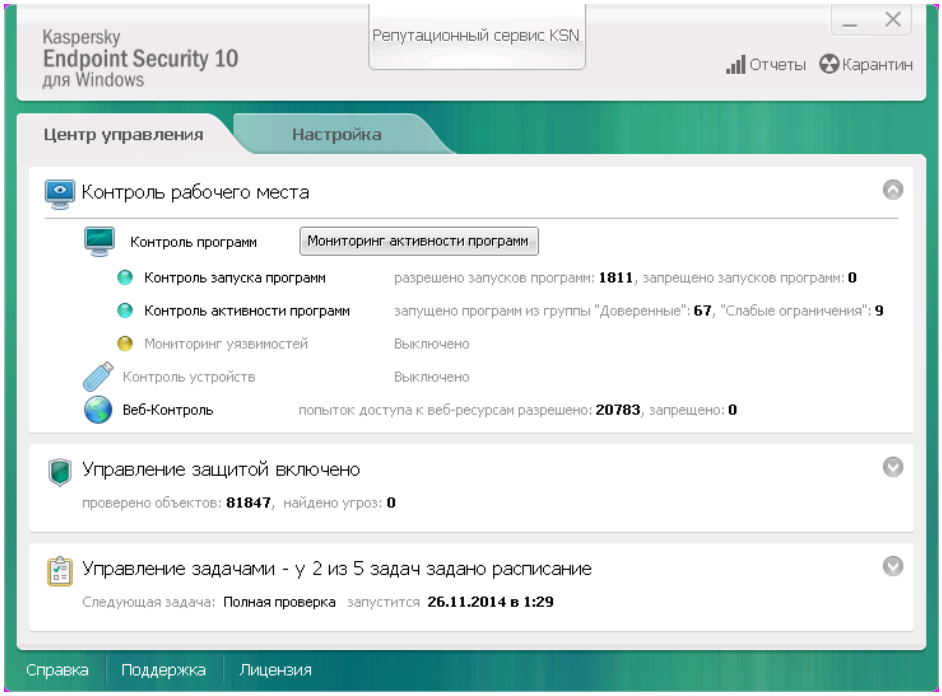
Фильтрация трафика антивирусным ПО

На примере ПО Kaspersky Internet Security.

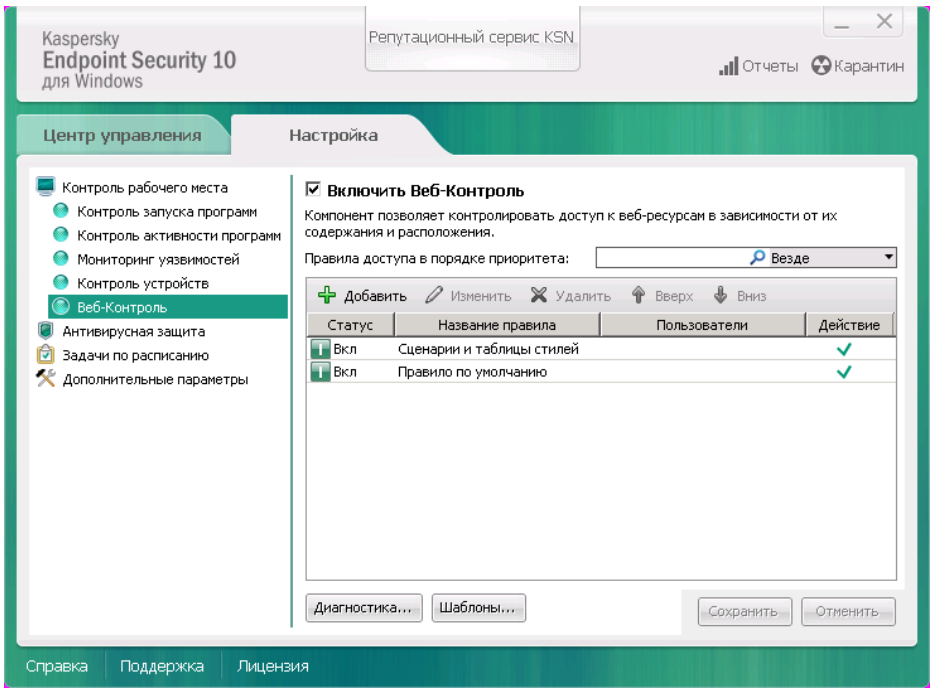
На компьютерах центров общественного доступа установлено программное обеспечение Kaspersky EndPoint Security (KES). Кроме защиты от вирусов и сетевых угроз, он обладает функцией «Веб контроль».

Настройка функции:

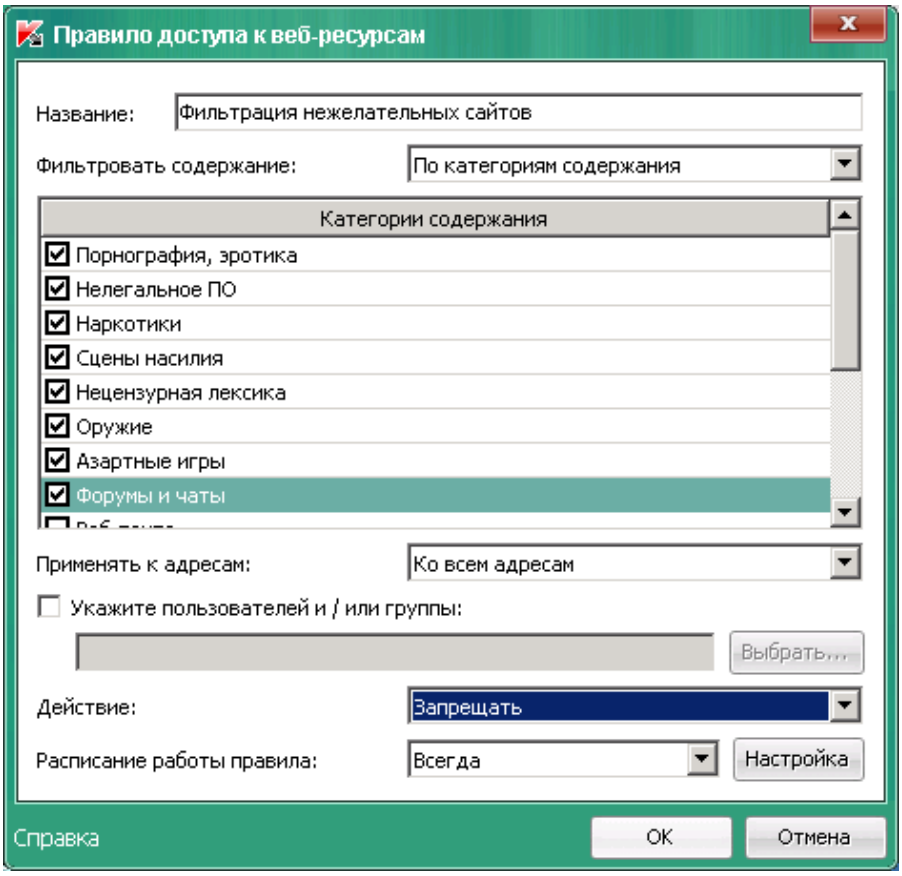
1. Откройте панель управления KES.



2.Найдите в меню строку «Веб контроль». Кнопкой «+» создайте новое правило.

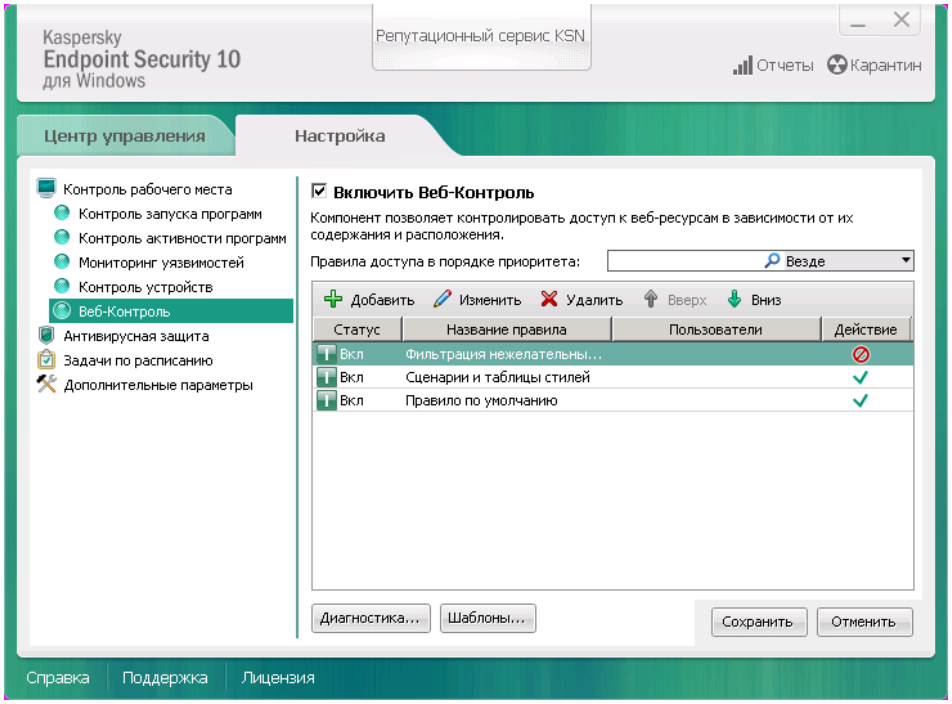


2. Введите название правила, выберите в «Фильтровать содержание» пункт меню «По категориям содержания». В поле «Применять к адресам» выберите «Ко всем адресам». В поле «Действие» выберите «Запрещать».



Сохраните форму.

Далее наше созданное правило передвиньте (кнопка «Стрелка Верх») на первую строчку:



Таким образом вы настроили фильтрацию по «черному списку». Список обновляется ежедневно. Результатом фильтрации будет красное окно в окне браузера, предупреждающее, что доступ закрыт.

Фильтрация трафика специализированным программным обеспечением

Дополнительно можно порекомендовать бесплатный интернет-фильтр для детей ИНТЕРНЕТ ЦЕНЗОР (http://www.icensor.ru/). Программа работает по «белому списку» и гарантирует защиту от опасных и нежелательных материалов. Разработчики утверждают, что более 1000000 Интернет-ресурсов доступно на рекомендуемом уровне фильтрации, в этом пространстве и будет работать пользователь.

В домашних условиях можно использовать программные решения для детей с элементами родительского контроля. Например, Norton Family (https://onlinefamily.norton.com).

Основные возможности:

- Контроль Интернета
- Контроль социальных сетей

- Контроль поиска
- Защита личной информации
- Контроль времени
- Мобильное приложение для родителей.

Фильтрация трафика с помощью браузера

Существуют специальные редакции браузеров и дополнения к обычным браузерам. Рассмотрим Интернет-обозреватель Гогуль (http://gogul.tv/). Этот детский браузер познакомит детей с современными информационными технологиями, а также оградит их от нежелательной, негативной информации. В сочетании со средствами «Родительского контроля» (правило: запускать только этот браузер) обеспечит хорошую защиту ребенка.

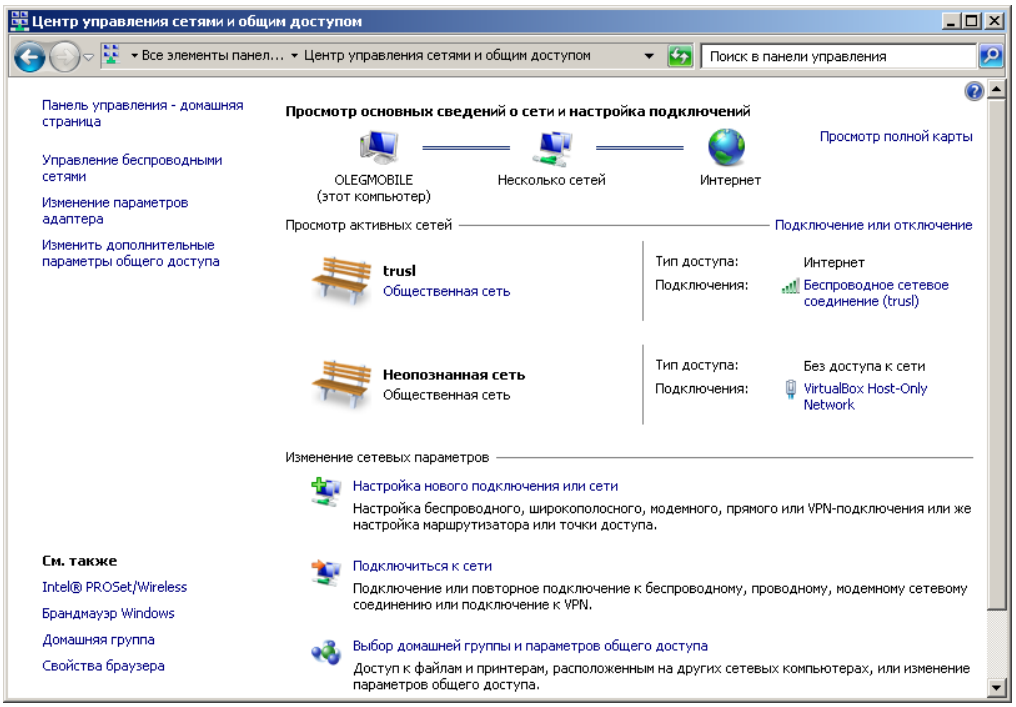
Фильтрация с использованием внешних ресурсов

Облачная фильтрация позволяет, не устанавливая дополнительного программного обеспечения, обеспечить защиту от вредоносных сайтов и нежелательного контента. Сервер, который обеспечивает защиту, находится в сети Интернет. Пользователь перенаправляет запросы, а сервис принимает решение о необходимости фильтрации. В случае необходимости защиты, пользователь видит в своем браузере специальную страницу с пояснением, почему был закрыт доступ.

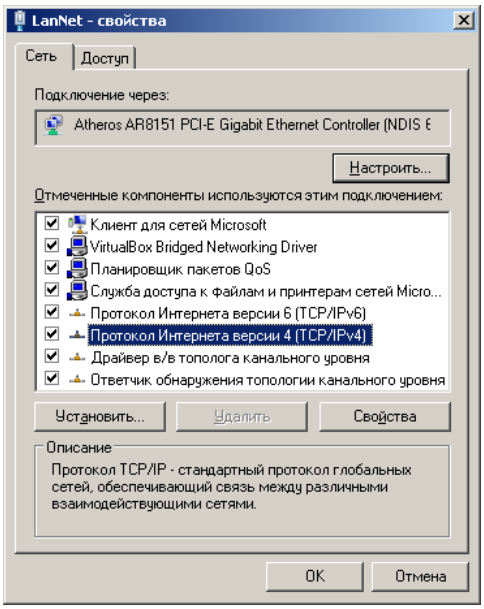
Рекомендуем 2 проекта: Яндекс.DNS (http://dns.yandex.ru/) и SkyDNS (https://www.skydns.ru).

Подготовка компьютера для облачной фильтрации

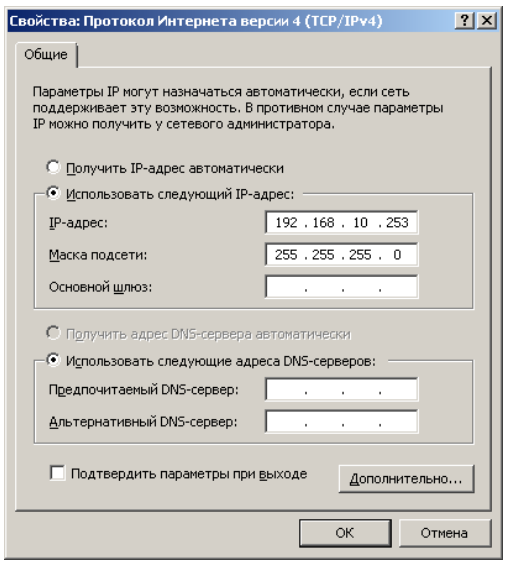
1. Открываем панель управления.
2. Запускаем программу «Центр управления сетями и общим доступом».



3. Выбираем «Изменение параметров адаптера». Находим значок «Подключение к локальной сети». В списке компонентов находим «Протокол Интернета версии 4 (TCP/IP)», нажимаем кнопку «Свойства».



4. Заполняем строку «Предпочитаемый DNS-сервер».



Яндекс.DNS (http://dns.yandex.ru/)

Всемирно известный поисковый сервис предлагает бесплатно защиту:

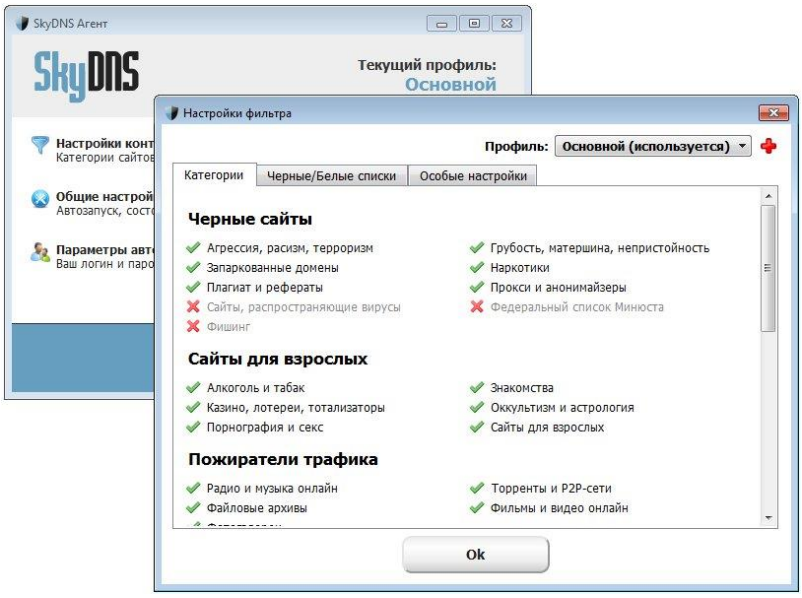
- от опасных сайтов
- от «взрослых» материалов
- от ботов.

Чтобы включить защиту, добавляем в строчки «Предпочитаемый DNS-сервер» и «Альтернативный DNS-сервер»: 77.88.8.7 и 77.88.8.3.

SkyDNS (https://www.skydns.ru)

Условно-бесплатный проект SkyDNS работает также как Яндекс.DNS и обеспечивает:

- Защиту от вредоносных сайтов
- Чистый интернет без баннеров и рекламы
- Управление доступом детей к интернет-сайтам
- Удобную программу для управления, позволяя открывать и закрывать доступ к группам сайтов:



Сервис бесплатен для домашнего использования (можно также настроить бесплатный доступ и для небольших сетей). Чтобы использовать SkyDNS необходимо зарегистрироваться в системе, указать ip адрес (система вам подскажет, если он меняется, то необходимо скачать с сайта специальную программу) и настроить строчку «Предпочитаемый DNS-сервер» в настройках вашего компьютера: 193.58.251.251.

Фильтрация средствами провайдера

Провайдеры, обслуживающие организацию, обязаны закрыть доступ к сайтам, включенным в списки Роскомнадзора. У большинства провайдеров есть специальные предложения по защите нежелательной информации. Эти продукты платные, но взамен пользователь получит ответственность профессиональной организации.