Интернет–фильтры

Интернет–фильтры позволяют ограничить доступ в Интернет. Такие программы блокируют доступ к определенным сайтам, например, порноресурсам, сайтам с информацией об оружии и наркотиках, а также контролируют время нахождения в сети.

1. **Интернет Цензор** – интернет-фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов. В основе работы программы лежит технология «белых списков», гарантирующая 100%-ную защиту от опасных и нежелательных материалов. Фильтр «Интернет Цензор» можно скачать бесплатно на официальном сайте http://www.icensor.ru/. Программа содержит уникальные вручную проверенные «белые списки», включающие все безопасные сайты Рунета и основные иностранные ресурсы. Программа надежно защищена от взлома и обхода фильтрации. «Интернет Цензор» может использоваться как в домашних условиях, так и в образовательных учреждениях, библиотеках, музеях, интернет-кафе и иных местах, где возможно предоставление несовершеннолетним доступа в Интернет.

2. **KinderGate Родительский Контроль 1.0.** Эта программа-фильтр (www.usergate.ru) предлагает 82 категории фильтрации веб-сайтов в 5 основных уровнях доступа (по умолчанию запрещен доступ к фишинговым ресурсам, сайтам с порнографическим контентам, а также к сайтам, содержащим вредоносный код). Самый высокий уровень фильтрации подразумевает, в числе прочего, запрет прокси-серверов, сайтов знакомств. Доступно создание расширенных правил, «черных» и «белых» списков для сайтов. Можно установить ограничение скачивания видео, звуковых файлов, изображений, архивов и EXE-файлов, документов. В программе реализован модуль морфологического анализа, позволяющий блокировать веб-страницы с нецензурной лексикой. Для ограничения времени, проводимого ребенком за компьютером, предусмотрен специальный инструмент «Расписание работы». Кроме этого, доступна статистика посещенных веб-ресурсов с указанием значений входящего и исходящего трафика, а также просмотр сообщений в сетях odnoklassniki.ru и vkontakte.ru.

3. Kaspersky Internet Security 2011 (www.kaspersky.ru) – антивирусная программа, которая защищает компьютер от вирусов и в состав которой входит модуль родительского контроля. Приложение способно не только ограничивать время, проводимое за компьютером, но и контролировать общение детей при использовании различных интернет-пейджеров, например, ICQ (поддерживаются клиентские приложения для сетей MSN, Jabber, IRC, Mail.ru и Yahoo). Действия ребенка в социальных сетях (FaceBook, MySpace, Twitter) тоже не останутся без внимания модуля родительского контроля, причем в определенных случаях можно не только создать «черный список» для

контактов, но и произвести запись сообщений. Для ограничения доступа к веб-ресурсам предусмотрено 14 категорий – родителям достаточно включить нужные. Если ресурс, к которому ребенок стремится получить доступ, не найден в базе данных, будет произведен эвристический анализ веб-страницы. Другой момент касается запрета передачи конфиденциальных данных, например, реквизитов банковской карты или домашнего адреса. Модуль родительского контроля позволит запретить загрузку следующих типов файлов: «Музыка», «Видео», «Программы» и «Архивы».

4. Интернет-фильтр «Кибер Папа» – бесплатная программа, которая ограничивает возможности ребенка выхода за пределы детского Интернета при использовании любого браузера. Скачать программу можно на официальном сайте http://cyberpapa.ru/. Программа работает по принципу «белого списка» и чрезвычайно проста в использовании. После ее инсталляции и включения фильтра ребенок может переходить только по страницам проверенных детских сайтов (блокируются также все статические и динамические объекты веб-страниц, не принадлежащие к списку проверенных детских ресурсов). Отключить фильтр могут только родители, используя известный им пароль от программы.

5. KidsControl – программа предназначена для ограничения доступа детей к нежелательным интернет-ресурсам, а также для контроля времени нахождения в сети. Скачать программу можно на официальном сайтеhttp://www.kidscontrol.ru/. С ее помощью можно установить ограничение доступа к нежелательным ресурсам по различным категориям – сайтам для взрослых, online-играм и казино, форумам, – указав галочкой на определенную категорию, и установить ограничение с помощью черного списка.

Настройка функции родительского контроля в операционной системе Microsoft Windows 7

Функции «родительского контроля» предусмотрены в операционной системе Windows 7, которая устанавливается на большинство новых компьютеров и ноутбуков. В частности Windows 7 дает возможность ограничивать время, которое ребенок проводит за компьютером: вы можете разрешить ему играть в игры или пользоваться социальными сетями 2-3 часа в день. Кроме того, операционная система от Windows позволяет устанавливать запрет на доступ детей к тем или иным играм или программам. Например, если вы не хотите, чтобы ребенок смотрел мультфильмы или фильмы, хранящиеся на жестком диске, можно запретить запуск мультимедийного плеера.

Источник: http://netnado.ru/metodicheskie-rekomendacii-po-kontrolyu-za-ispolezovaniem-neso/page-1.html

Для того чтобы активировать функцию родительского контроля в Windows 7:

1. Нажмите ***Панель управления/Учетные записи пользователей и семейная безопасность/Родительский контроль***. Щелкните на учетную запись пользователя, чью работу за компьютером вы хотели бы контролировать. Если учетной записи нет, щелкните ***Создать новую учетную запись*** (рис. 1).

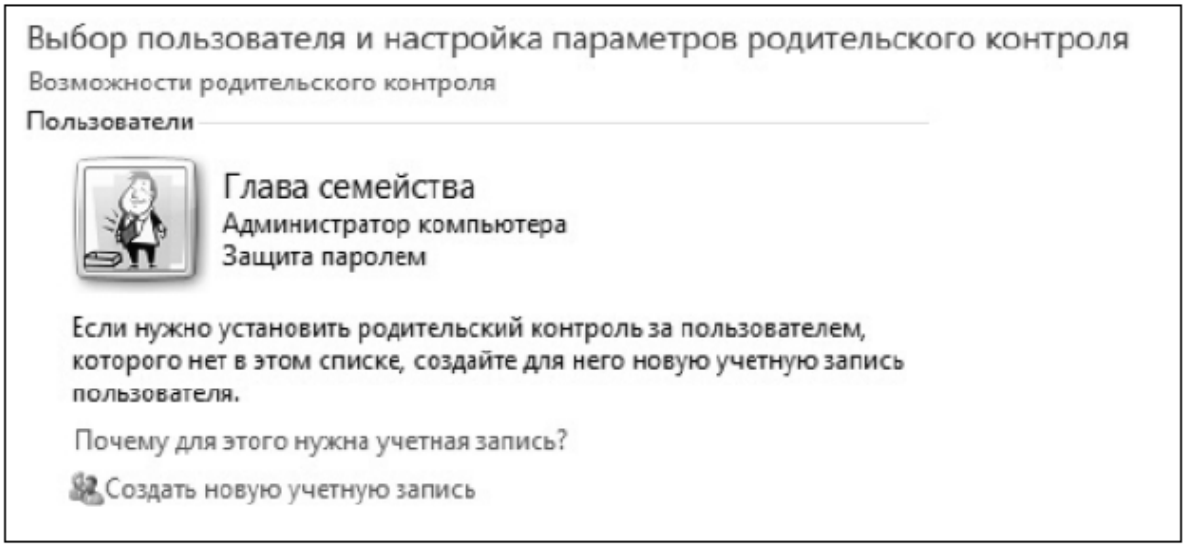


Рис. 1. Создание учетной записи

2. В появившемся окне в настройке ***Родительский контроль*** выберите ***Включить, используя текущие параметры***. Теперь вы можете установить ограничения по времени использования компьютера, а также играм и программам, которые можно запускать (рис. 2).

Рис. 2. Установка ограничения по времени

3. Для того чтобы установить ограничения времени использования компьютера, щелкните ***Ограничения по времени***, в появившемся расписании выделите мышью дни и часы, в которые разрешается использовать компьютер.

4. Для того чтобы разрешить или блокировать конкретную программу, щелкните ***Разрешение и блокировка конкретных программ***.

Настройка интернет-цензора

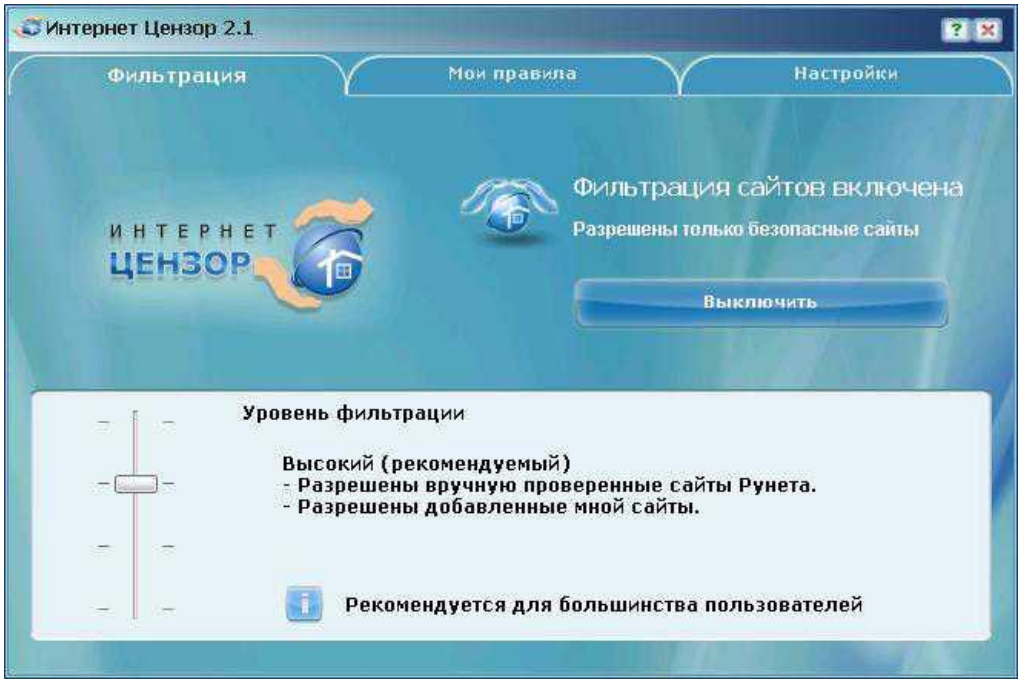
Чтобы открыть управляющее приложение, курсором мыши выберите изображение программы в панели инструментов и сделайте клик левой клавишей.

Перед вами появится окно с вводом пароля:

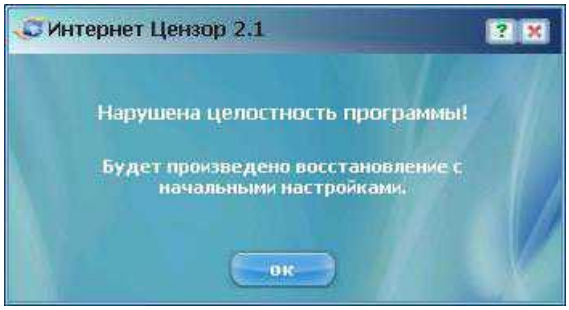
Введите пароль, который вы указали при установке программы.

Если вы забыли пароль, кликните по надписи «Напомнить пароль» для восстановления пароля на электронную почту.

Если введен правильный пароль, откроется окно программы:



Если значок свернутой программы мигает, меняя цвет с синего на красный, то это сигнал о том, что была попытка взлома программы (ребенок пытался удалить или вывести из строя «Интернет Цензор»). В этом случае на почтовый адрес, введенный вами при установке программы, будет отправлено соответствующее оповещение. Если вы кликнете на значок приложения, то откроется окно:



Следуйте инструкции, которую вы увидите в окне программы.

Управляющее приложение поможет вам настроить программу «Интернет Цензор» под конкретные потребности.

Интерфейс приложения содержит 3 вкладки:

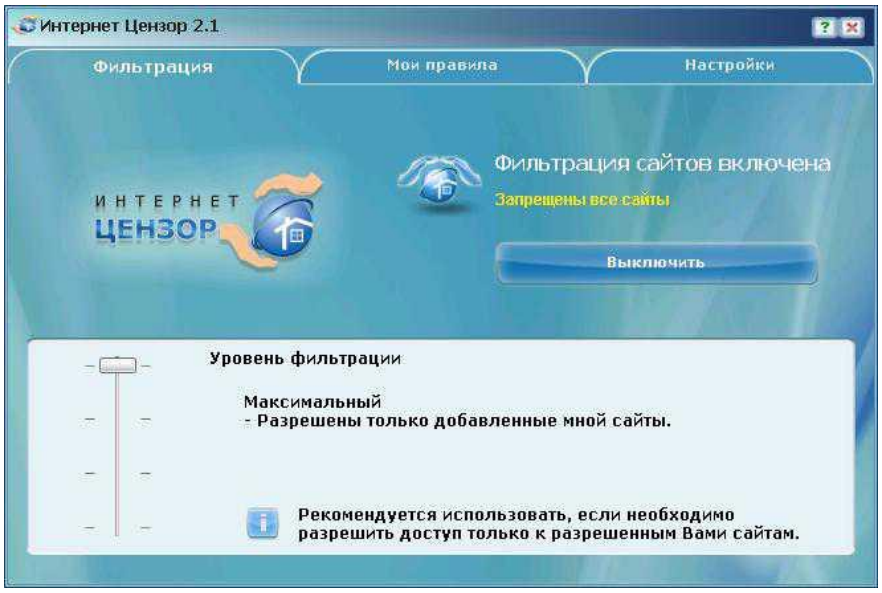
- Фильтрация
- Мои правила
- Настройки

Рассмотрим каждую из вкладок подробнее.

Вкладка «Фильтрация»

На этой вкладке вы можете управлять уровнями фильтрации. Каждый следующий уровень фильтрации (движение ползунка сверху вниз) является расширением предыдущего. Рассмотрим каждый уровень отдельно.

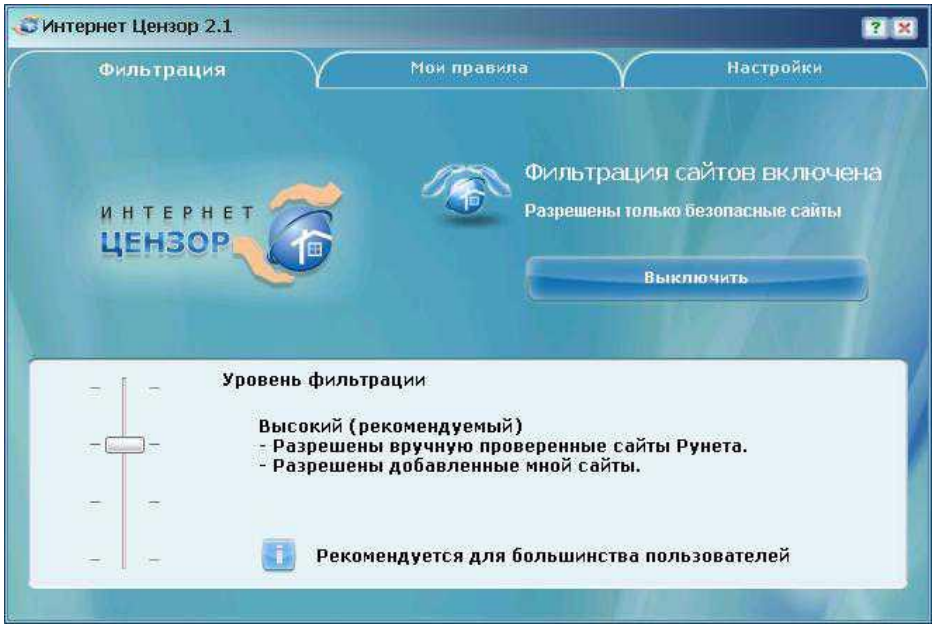
Максимальный уровень:



На этом уровне фильтрации разрешены только добавленные вами в «белый список» сайты на вкладке «Мои правила». Все остальные сайты Интернета будут блокироваться программой.

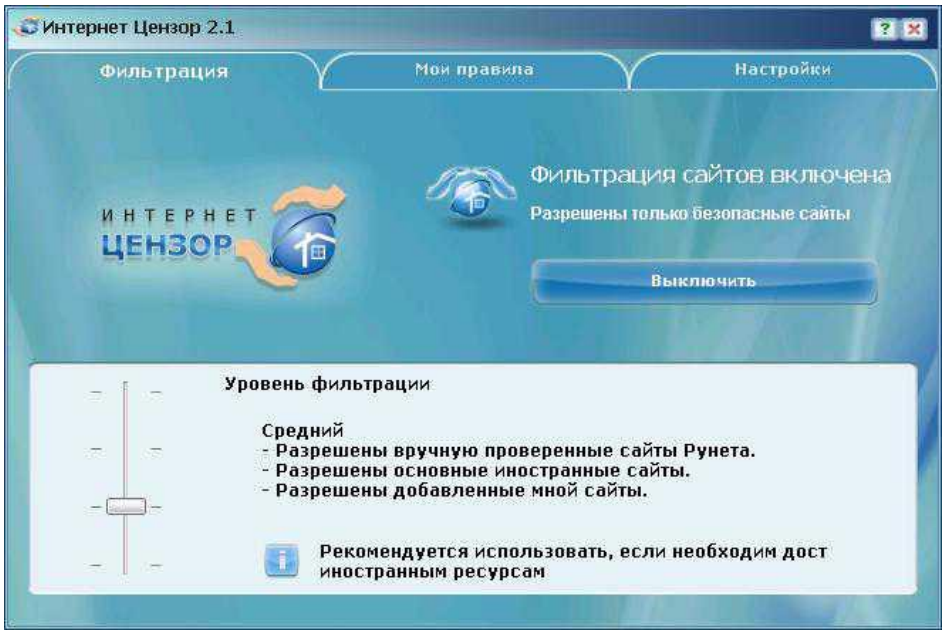
Высокий уровень:

Источник: http://netnado.ru/metodicheskie-rekomendacii-po-kontrolyu-za-ispolezovaniem-neso/page-1.html



На этом уровне, кроме разрешенных вами сайтов, разрешена вручную проверенная база русского Интернета. Данный уровень является оптимальным, и мы рекомендуем использовать его.

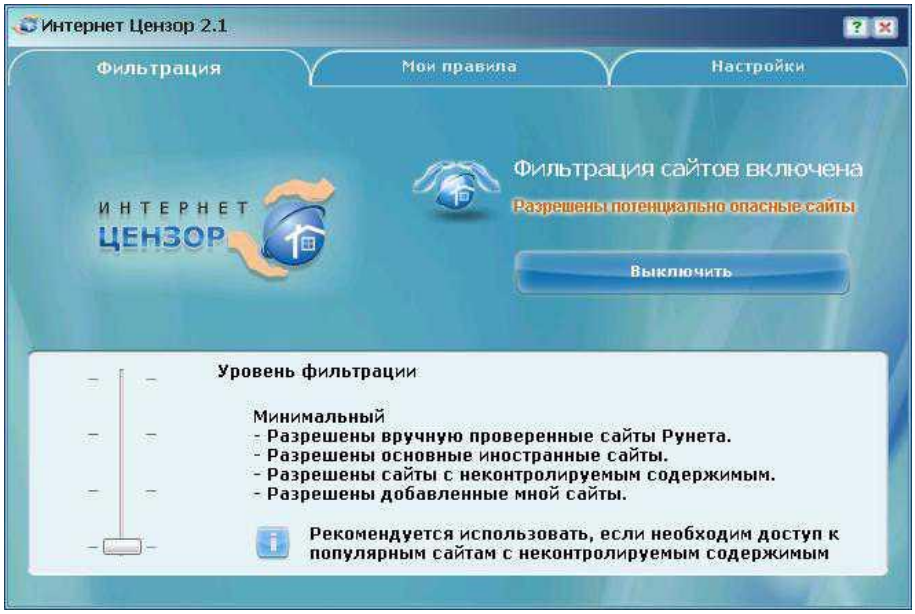
Средний уровень:



На этом уровне то же, что и на **Высоком уровне** плюс база основных иностранных сайтов.

Минимальный уровень:

Источник: http://netnado.ru/metodicheskie-rekomendacii-po-kontrolyu-za-ispolezovaniem-neso/page-1.html



На этом уровне разрешено то же, что и на **Среднем уровне** плюс ресурсы с неконтролируемым содержимым:

- социальные сети,
- файлообменники и файлораздачи, в том числе сайты пиринговых сетей,
- фото- и видеохостинги (youtube.com, rutube.ru и т.д.),
- блоги (кроме профессиональных и тематических, например, allboxing.ru),
- чаты,
- онлайн-игры.

Вкладка «Мои правила»

Источник: http://netnado.ru/metodicheskie-rekomendacii-po-kontrolyu-za-ispolezovaniem-neso/page-1.html

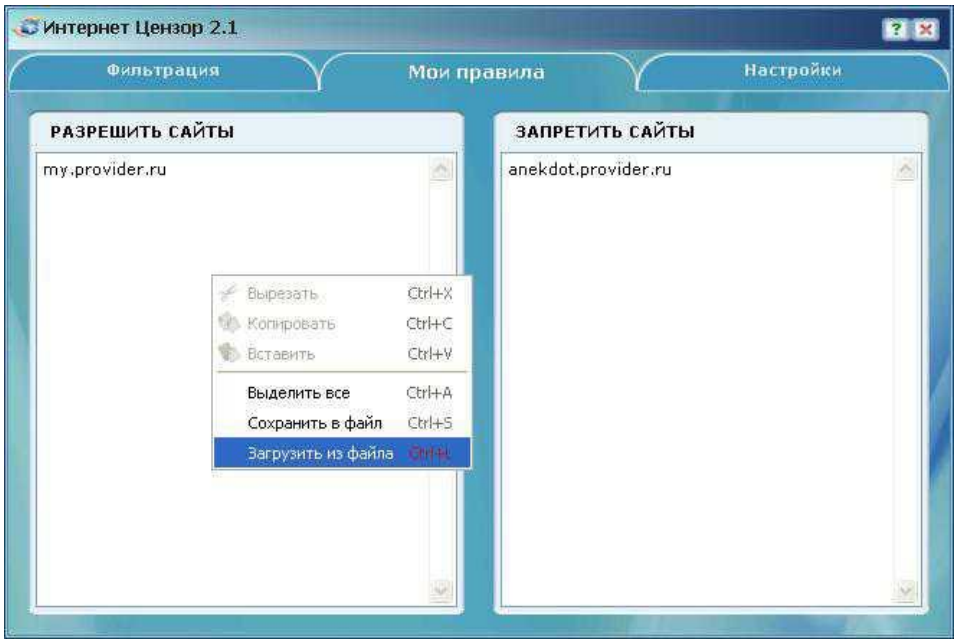
На этой вкладке вы можете указать адреса интернет-сайтов, к которым должен быть разрешен или запрещен доступ. Внесенные вами изменения вступят в действие немедленно. Если введенные вами данные или часть данных изменит свой цвет на красный, то это значит, что была допущена ошибка в тексте. В этом случае вам следует сделать необходимые исправления.

Сайты, которые вы вносите в свои «черный» и «белый» списки, рекомендуется сохранять также и в отдельном текстовом файле. Если вам придется переустановить программу, все настройки сбросятся. В этом случае вы просто скопируете список ресурсов из текстового файла в списки программы.

Если вы захотите сохранить данные из «черного» или «белого» списка в текстовый файл, то при клике правой кнопкой мыши в области списка доступно меню с пунктом **Сохранить в файл**:

Источник: http://netnado.ru/metodicheskie-rekomendacii-po-kontrolyu-za-ispolezovaniem-neso/page-1.html

Вы также можете загрузить сайты из текстового файла в список, выбрав пункт **Загрузить из файла**:



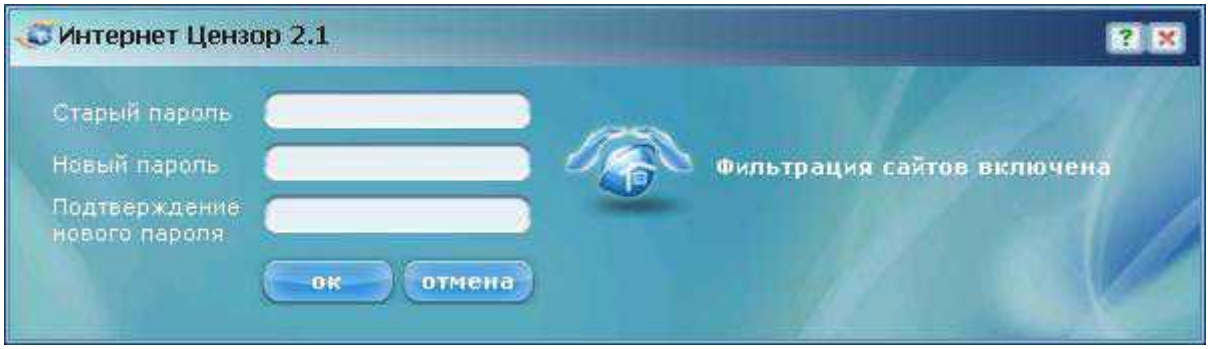
Вкладка «Настройки»

Источник: http://netnado.ru/metodicheskie-rekomendacii-po-kontrolyu-za-ispolezovaniem-neso/page-1.html

На этой вкладке вы можете:

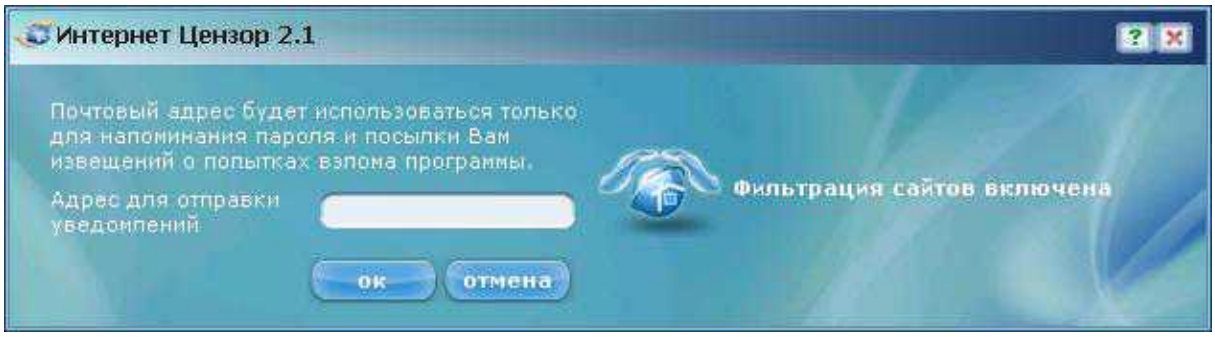
- проверить обновления базы компании,
- изменить текущий пароль,
- изменить введенный вами ранее почтовый адрес, который используется для получения вами уведомлений о работе системы,
- наложить дополнительный запрет на активность в сети.

Если вы захотите изменить старый пароль, перед вами откроется окно:



Введите сначала старый пароль, а затем новый. Подтвердите новый пароль и нажмите кнопку «ОК».

Окно смены почтового адреса выглядит так:



Введите в поле тот адрес электронный почты, по которому вы хотите в дальнейшем получать сведения о работе программы. Напоминаем, что этот почтовый адрес используется исключительно для отправки на него уведомлений о попытке взлома программы на вашем компьютере.

Запрет на дополнительную активность в сети. В этом случае вы можете запретить:

- использование интернет-пейджеров, таких как программы обмена мгновенными сообщениями типа ICQ (а также других клиентов сети ICQ, например, QIP), Mail.ru Агент;
- использование клиентов файлообменных сетей, например, BitTorrent.

Настройка безопасности в поисковых системах

Родителям следует знать, что у популярных поисковых систем и почтовых служб существуют специальные защитные функции, которые с легкостью можно настроить самостоятельно. В большинстве популярных поисковых систем есть опция так называемого безопасного поиска, которая предполагает фильтрацию сайтов сомнительного содержания в поисковой выдаче. При активации этой функции поисковые машины производят фильтрацию не только по выдаче сайтов, но и по выдаче картинок на любой запрос. У почтовых сервисов можно настроить специальные фильтры, чтобы блокировались все сообщения с определенными параметрами или словами.

В Google фильтрация результатов поиска включается в разделе «Настройки

поиска», который появляется при клике мыши на значок шестеренки в правом верхнем углу заглавной страницы www.google.ru. В меню «Безопасный поиск» установите режим «Строгая фильтрация», который предусматривает отсеивание непристойных картинок и текста. Не забудьте нажать кнопку «Сохранить настройки».

Применять фильтр к результатам поиска позволяет и Яндекс. В разделе «Настройки – Остальное» есть пункт «Настройка результатов поиска», а в нем – меню «Фильтрация страниц».

Службы помощи

Фонд поддержки детей, находящихся в трудной жизненной ситуации (http://www.fond-detyam.ru) – общероссийский проект «Телефон доверия». По телефону 8-800-2000-122 предоставляются психологические консультации по проблемам насилия и принуждения к сексуальной эксплуатации, оказывается помощь жертвам подобных преступлений, а также консультации по всем психологическим проблемам детей и подростков. Все консультации и звонок на телефонный номер Линии помощи бесплатны; консультации предоставляются круглосуточно. На сайте Фонда можно получить консультации, вступив в переписку со специалистами Фонда.

На сайте ***Я – родитель*** (http://www.ya-roditel.ru) размещены полезные материалы, адресованные родителям, обеспокоенным интернет-угрозами детям.

На сайте Центра безопасного Интернета в России http://www.saferunet.ru необходимо кликнуть на красный баннер «горячая линия» и сообщить о противоправном контенте. На сайте размещена линия помощи – консультации по вопросам интернет-угроз. По всем вопросам, связанным с безопасным использованием Интернета, – посредством тематических веб-форм обращений на сайте или через электронную почтуhelpline@saferunet.ru; по общим вопросам, в том числе по вопросам, связанным с безопасным использованием Интернета, – посредством тематических веб-форм на специальном сайте http://www.psyhelpline.ru.

Линия помощи «Дети – онлайн» http://www.detionline.com – служба телефонного и онлайн-консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками Интернета и мобильной связи.

Обратиться на линию помощи можно по телефону 8-800-250-00-15 (звонить с 9.00 до 18.00 по рабочим дням, время московское, звонки по России – бесплатные), по электронной почте helpline@detionline.com.

Список терминов

Блог (англ. blog, интернет-журнал событий, интернет-дневник, онлайн-дневник) — веб-сайт, основное содержимое которого – регулярно добавляемые записи (посты), содержащие текст, изображения или мультимедиа.

Браузер (от англ. *Web browser)* – программное обеспечение для просмотра веб-сайтов, то есть для запроса веб-страниц, их обработки, вывода и перехода от одной страницы к другой.

Видеохостинг – сайт, позволяющий загружать и просматривать видео в браузере, например, через специальный проигрыватель.

Вишинг – разновидность фишинга – распространенного сетевого мошенничества, при котором клиенты какой-либо платежной системы получают сообщения по электронной почте якобы от администрации или службы безопасности данной системы с просьбой указать свои счета, пароли и т.д. При этом ссылка в сообщении ведет на поддельный сайт, на котором и происходит кража информации. Сайт этот уничтожается через некоторое время, и отследить его создателей в Интернете достаточно сложно.

Интернет-мошенничество или кибермошенничество – один из видов киберпреступления, целью которого является обман пользователей.

Кибербуллинг – виртуальный террор, чаще всего подростковый.

Контент (от англ. content – содержание) – абсолютно любое информационно значимое, содержательное наполнение информационного ресурса или веб-сайта. Контентом называются тексты, мультимедиа, графика.

Социальная сеть – платформа, онлайн-сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений.

Фарминг – процедура скрытного перенаправления жертвы на ложный IP-адрес. Для этого может использоваться навигационная структура.

Фишинг – вид интернет-мошенничества, основанный на незнании пользователями норм сетевой безопасности, целью которого является получение доступа к конфиденциальным данным – логинам и паролям. Фишинг-атаки проводятся через электронную почту, всплывающие сообщения и ссылки на фишинговые веб-сайты с целью обманным путем выявить у получателя личную информацию, часто финансового характера.

Нигерийские письма **–** распространѐнный вид мошенничества, получивший развитие с появлением массовых рассылок по электронной почте (спама).