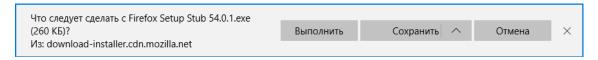
Шаг 1: Установка браузера Firefox в ОС Windows 10

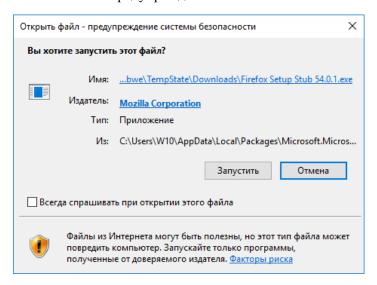
Открываем браузер Microsoft Edge (см. первый рисунок ниже) и загружаем Firefox по ссылке: https://www.mozilla.org/ru/firefox/new/?scene=2



Внизу появится вплывающее окно загрузки. Нажимаем кнопку «Выполнить».



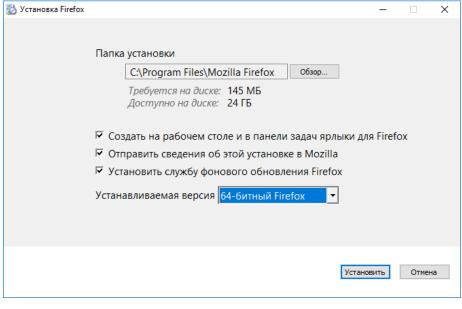
Появится окно предупреждения системы безопасности. Нажимаем кнопку «Запустить».

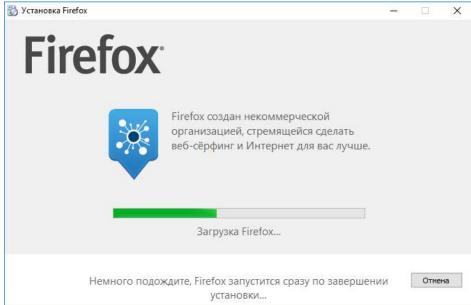


Внизу появится вплывающее окно загрузки. Нажимаем кнопку «Выполнить».

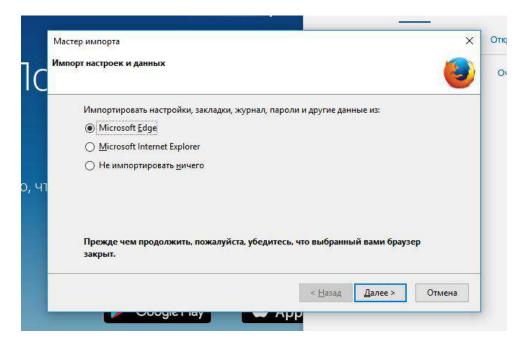
После этого нажимаем на настройки установки и выбираем 64-битную версию для Firefox. Нажимаем «Установить».



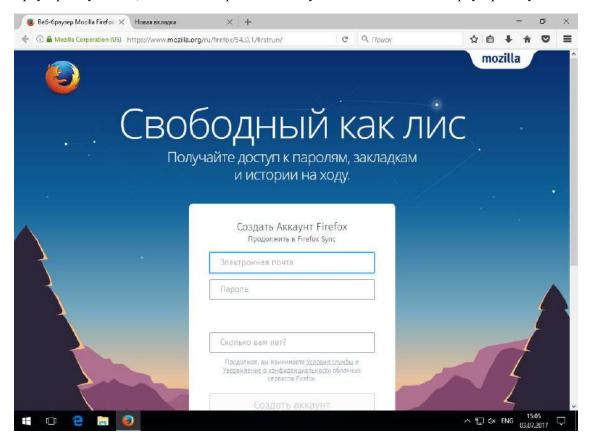




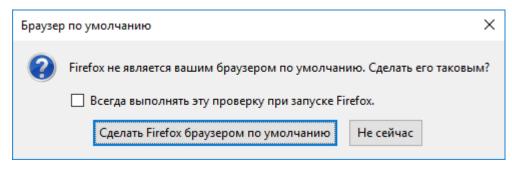
После установки в окне импорта настроек и данных выбираем пункт «Microsoft Edge», который был ранее браузером по умолчанию. Подтверждаем наш выбор нажатием кнопки «Далее».



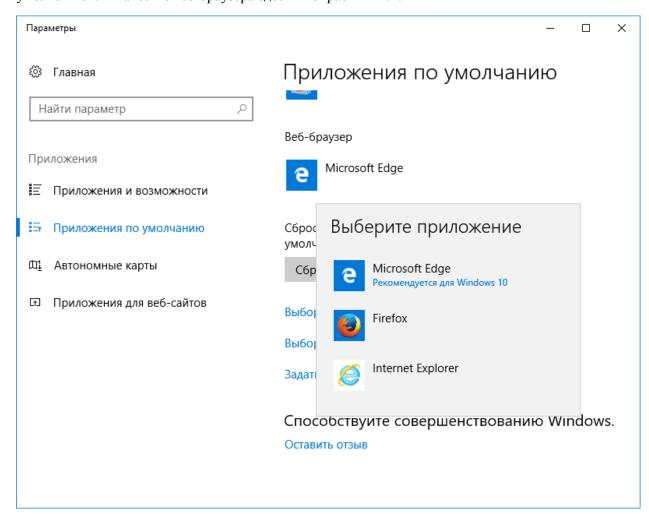
Браузер запустился, но нам ещё предстоит его установить в качестве браузера по умолчанию.



При появлении этого окошка жмем кнопку «Сделать Firefox браузером по умолчанию».

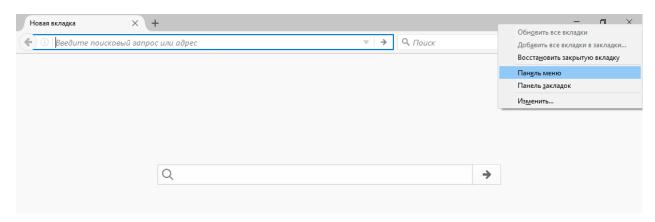


После этого нас перенаправит ОС на окно параметров в пункте меню «Приложения по умолчанию». В качестве веб-браузера здесь выбираем «Firefox».

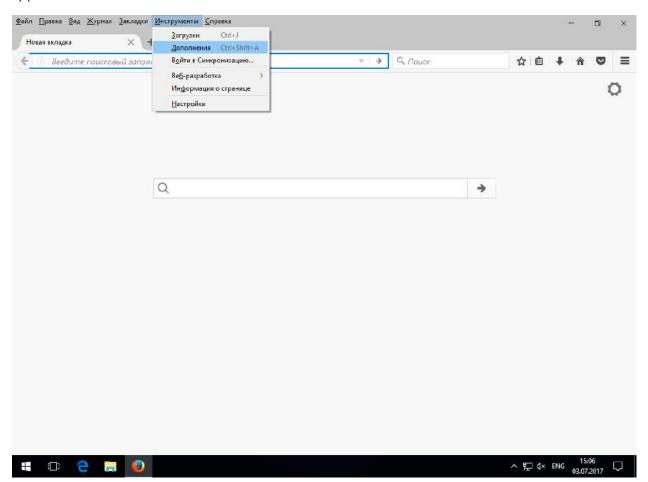


Регулируем окно Firefox. Правым кликом на серой верхней полосе окна открываем контекстное меню регулировки окна браузера и выбираем «Панель меню».

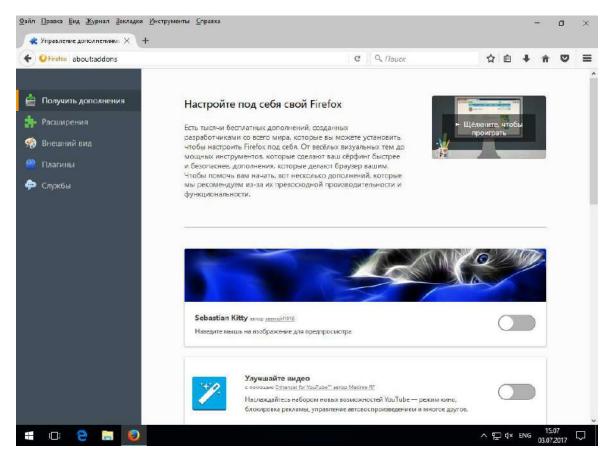
Шаг 2: Настройка браузера Firefox и установка начальных дополнений



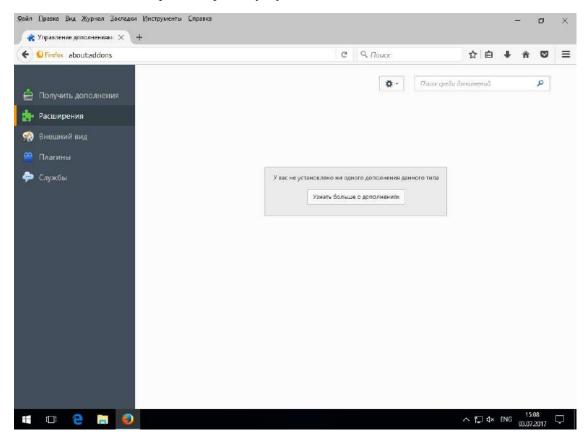
Панель меню отобразилось. Нажимаем на пункт панели «Инструменты» и выбираем «Дополнения».



Открылась вкладка установки и настройки дополнений. Но из них нам нужно установить расширения. Нажимаем на кнопку «Расширения».

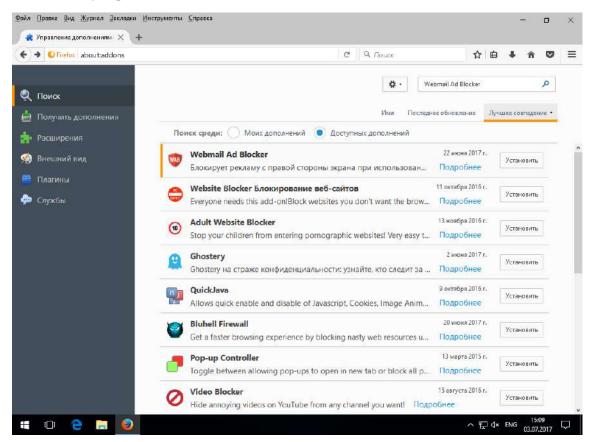


У нас ещё нет ни одного установленного расширений. Но его можно найти при помощи поля поиска дополнений в правом верхнем углу.

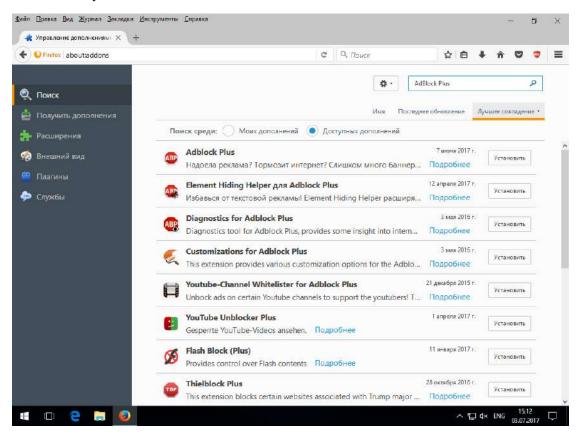


Первым делом установим дополнения, блокирующие рекламу. При установке некоторых расширений необходимо перезагружаться по требованию установщика, нажав на гиперссылку «Перезагрузить сейчас».

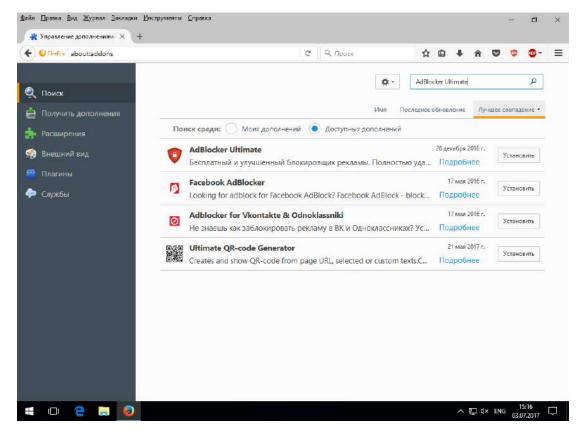
Вводим «Webmail Ad Blocker», жмем «Enter» и устанавливаем соответствующее дополнение, нажав кнопку справа «Установить».



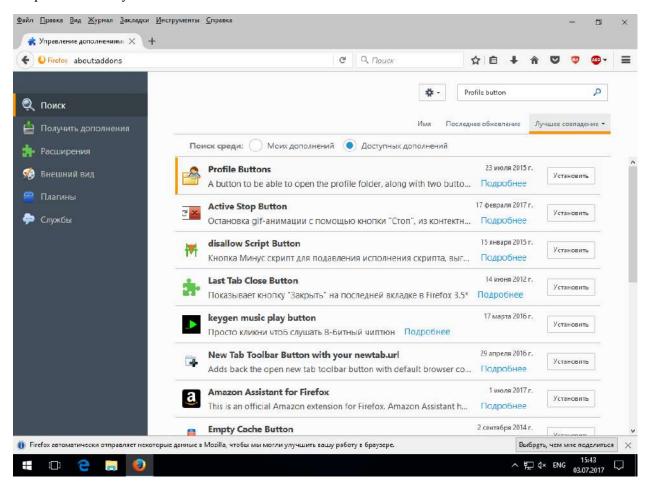
Аналогично устанавливаем «AdBlock Plus».



Также и «AdBlocker Ultimate»



Проделываем установку дополнения «Profile Button», благодаря которому вправо от адресной строки появится кнопка нашего пользовательского профиля браузера, на которую при нажатии мы откроем его папку.

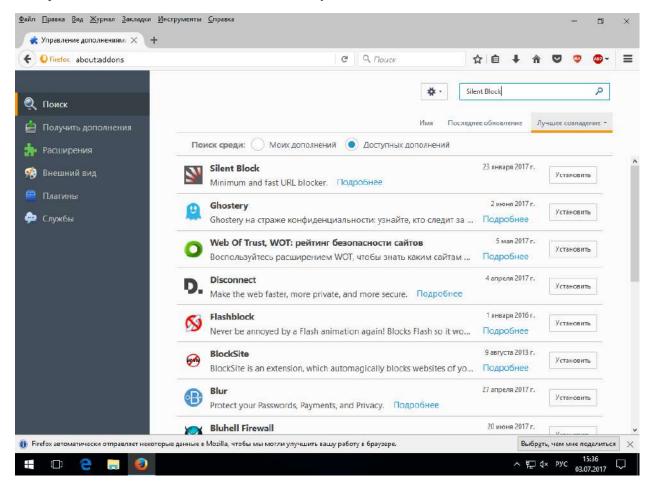




Шаг 3: Установка дополнений браузера Firefox, блокирующих нежелательные сайты, и браузерной утилиты MozBackup

Здесь необходимо учесть то, что для браузера пользователя старше восемнадцати лет необходим специальный комплекс дополнений.

Набираем в поиске дополнений «Silent Block» и устанавливаем его.



Нажимаем на кнопку профиля справа от адресной строки и создаем в папке профиля файл «contentblock-regex.txt», нажимая правым кликом на пустую область проводника Windows и выбрав пункт «Создать» - «Текстовый документ».

В этом текстовом документе указываются шаблоны блокирования текста в адресной строке Firefox для Silent Block, который осуществляет блокировку нежелательных адресов.

Для примера вводим в содержимое contentblock-regex.txt шаблон, который блокирует открытие поисковых страниц в Яндексе далее четырех страниц:

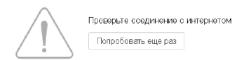
 $https\W\W\wardex.ru.+text=.+.p=[1-9][0-9]$

 $https\W\W$ yandex.ru.+text=.+.p=[4-9]

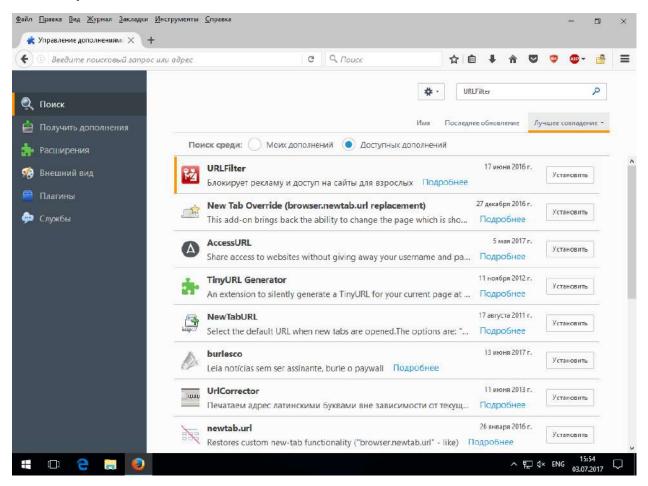
Проведём проверку, набрав в строке поиска Яндекса запрос «regexp». Должен получится результат, как на нижнем снимке.

Аналогично можно создать текстовый файл шаблонов для игнорирования блокировки некоторых сайтов «contentblock-whitelist-regex.txt» для Silent Block. Для создания текстовых шаблонов используется синтаксис регулярных выражений, с которым можно ознакомиться из специальной памятки: http://www.exlab.net/tools/sheets/regexp.html Сайт их тестирования находится здесь: http://regexr.com/

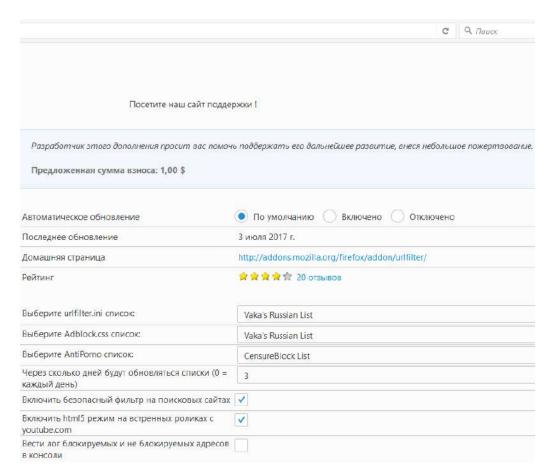




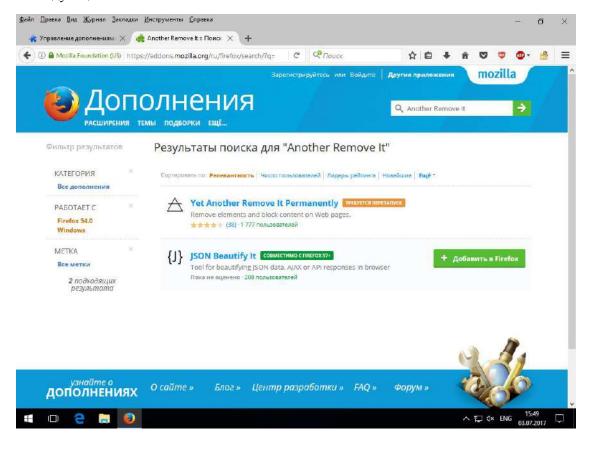
Займемся установкой дополнения URLFilter. Устанавливаем его.



Заходим в список установленных расширений, нажав на кнопку «Расширения». Жмем на кнопку дополнения URLFilter «Настройки». Здесь делаем выбор списков блокировки нежелательных сайтов, как на ниже приведенному снимке экрана.

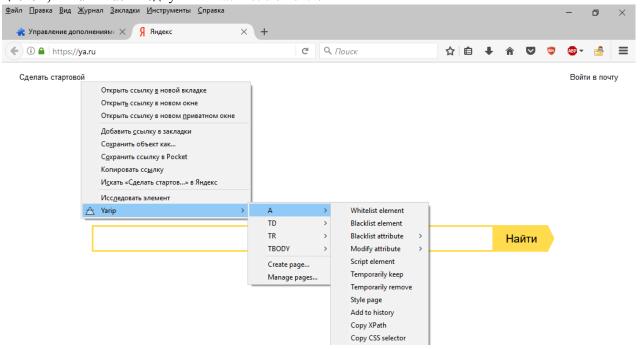


Устанавливаем дополнение «Yet Another Remove It Permanently», блокирующее назойливые элементы веб-страниц. Если не ищется оно стандартным способом, описанным выше, набираем в адресной строке https://addons.mozilla.org и набираем в правом верхнем поле «Another Remove It» с последующим нажатием клавиши «Enter».

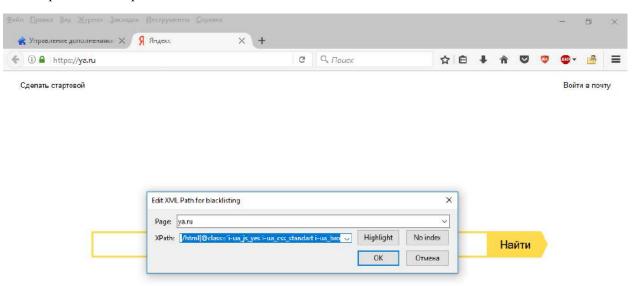


Это дополнение функционирует следующим образом: при нажатии на элемент правым кликом мыши в контекстном меню имеется пункт «Yarip», откуда мы можем отредактировать правило отображения элемента некоторой веб-страницы.

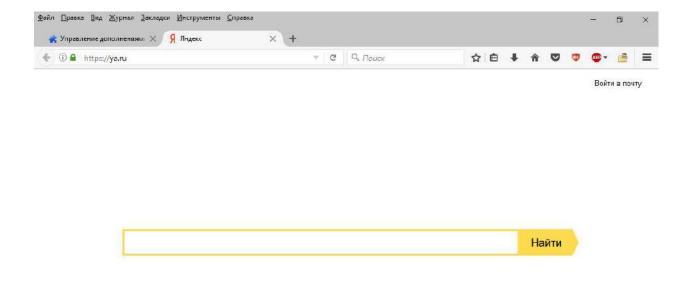
Заходим на уа.ru и для примера заблокируем отображение ссылки «Сделать стартовой» из левого верхнего угла страницы. Правым кликом активизируем контекстное меню, выбираем пункт «Yarip», выделяем элемент «А» (для подсказки выделения объектов дополнение их обводит синим цветом) и нажимаем подпункт «Blacklist element».



Подтверждаем выбор кнопкой «ОК» на появившемся окне.



После этого видно, что элемент веб-страницы успешно скрыт дополнением.



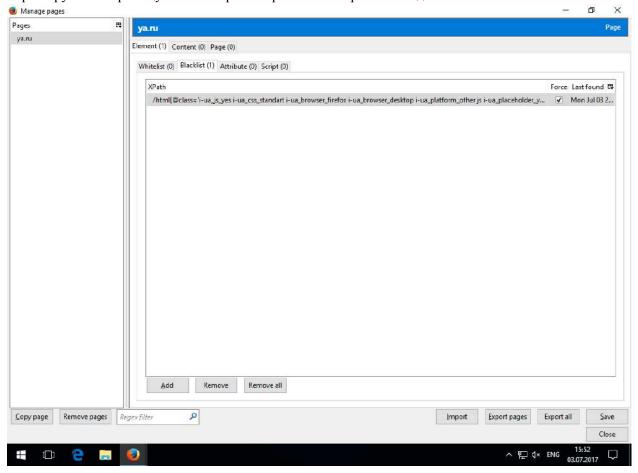
Яндекс



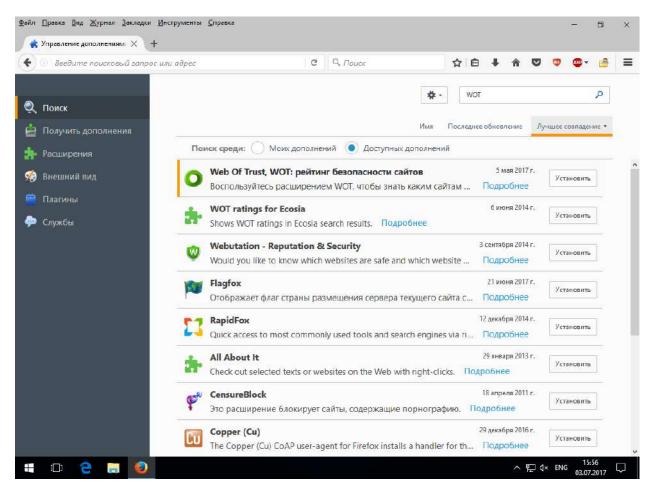
При этом правила Yarip можно удалять или редактировать. Нажимаем на меню «Инструменты», заходим в меню дополнения и нажимаем пункт «Mange pages...».



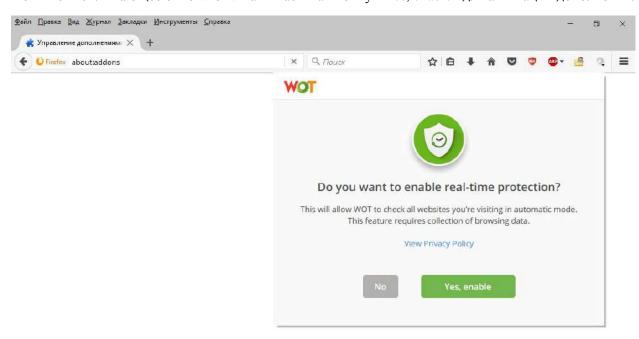
Как видно из этого окна, наше правило по домену «уа.ru» есть в базе Yarip. Удаляем его и перезагружаем страницу. Она теперь отображается в прежнем виде.



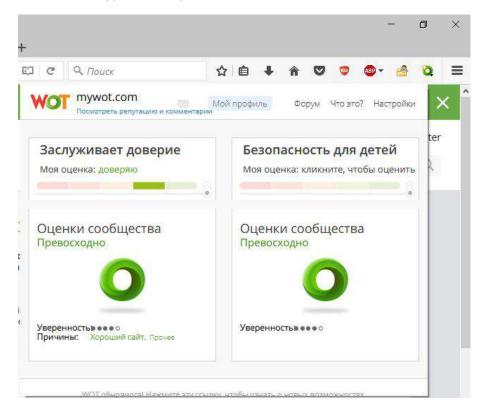
Следующее дополнение — это система оценивания сайтов «WOT - Web of trust». Ищем его и установщик попросит перезагрузить Firefox — перезагружаем.



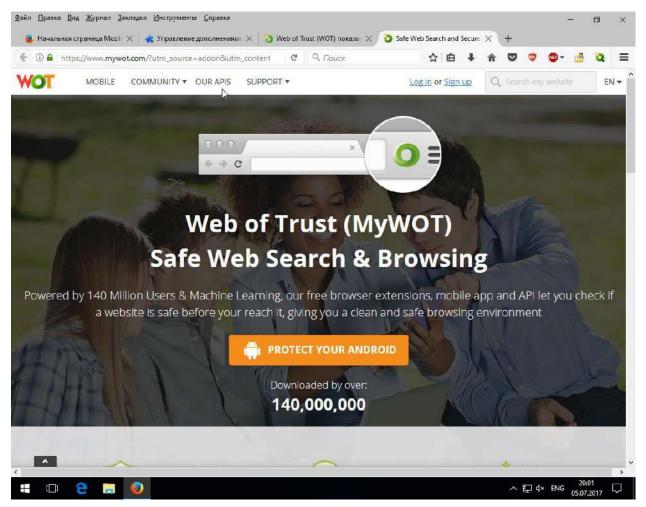
Появится всплывающее окно WOT. Нажимаем на кнопку «Yes, enable» для активации дополнения.



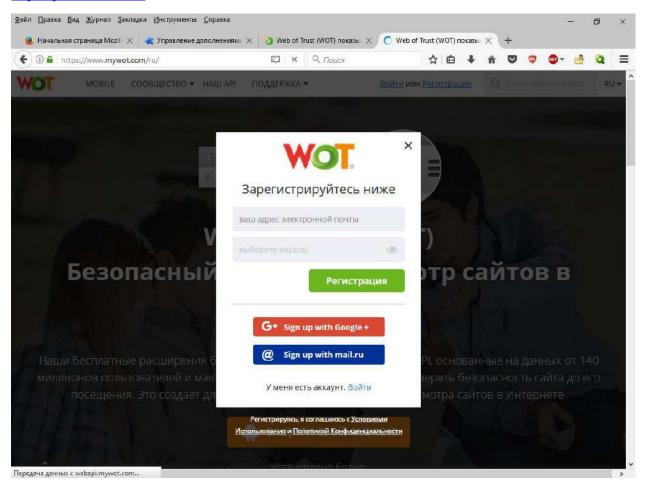
Вот как выглядит окно оценивания сайтов от WOT. Жмем на его логотип из левого верхнего угла.



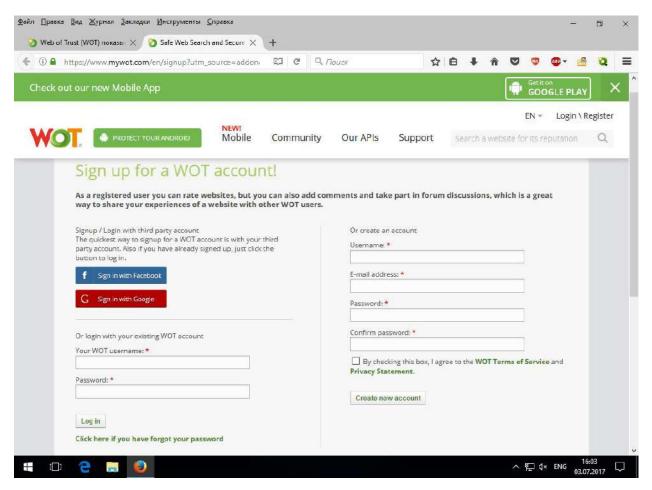
Откроется заглавная страница веб-сайта дополнения. В правом верхнем углу выбираем русский язык и регистрируемся по ссылке «Регистрация».



Регистрация в дополнении осуществляется через адрес электронной почты. Здесь конечно надо иметь в виду, что на вашу учетную запись могут вести досье во время использования любого сервиса, и WOT не исключение (http://www.pcworld.com/article/3139814/software/web-of-trust-browser-extensions-yanked-after-proving-untrustworthy.html). Поэтому регистрируемся с помощью временной электронной почты (https://crazymailing.com) или почтовой учётной записи сервиса https://protonmail.com.



В англоязычном интерфейсе регистрация выглядит более информативно.



В настройках дополнения, вызываемых с помощью одноименного пункта меню «WOT» - «Инструменты», можно определить нужно ли блокировать сайты с отрицательной репутацией.

Гид по Web of Trust перечисляет достаточно широкий функционал дополнения. Плюс дополнения в том, что фишинговые и вредоносные сайты достаточно быстро и автоматически попадают в черный список дополнения. Минус в том, что на некоторые сайты, не содержащие нежелательную информацию или вирусы, может вестись целенаправленное негативное рейтингование, и тут приходится с помощью этого дополнения его добавлять в свой зеленый список.

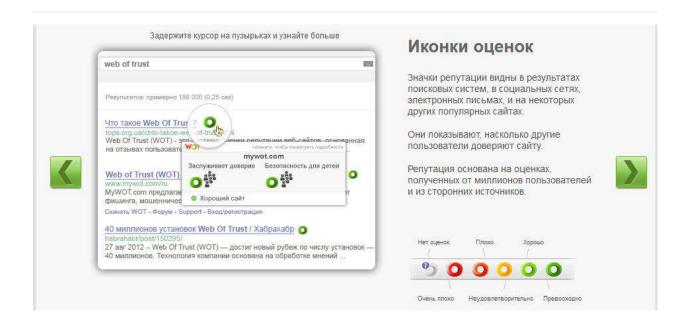


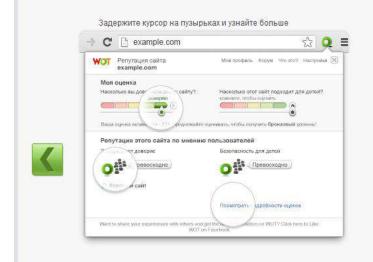
Warning notifications

Show advanced settings

Select the level of protection: Normal (Recommended) Shows different type of warnings depending on the type of threat. Select the type of warning Warning pop-up only (Recommended) Warning pop-up and blocking of sites with poor reputation Light Shows only a small notification when a threat is identified. Off No warnings shown. ✓ Parental control Reputation icons next to links Always (Recommended) Shows all types of icons next to links (red, yellow and green). Only icons with poor reputation Shows only icons indicating a poor reputation (red) Off No icons shown. Real-time Protection On (Recommended) Proactive protection against online threats. Highlights suspicious links. View Privacy Policy

Manual Mode - no active protection, only requests by demand.





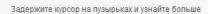
Окно рейтинга

Вы можете внести свой вклад, оценивая сайты в соответствии с вашим опытом.

Таким образом вы можете поделиться своими знаниями и сделать Интернет безопасней для других.

Пожалуйста, оценивайте только знакомые вам сайты.





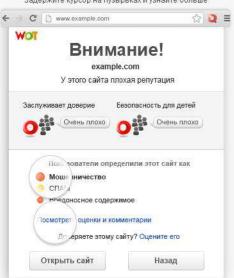


Оценочная карта

У каждого сайта есть своя оценочная карта WOT, которая даёт подробную информацию о репутации сайта



Задержите курсор на пузырьках и узнайте больше



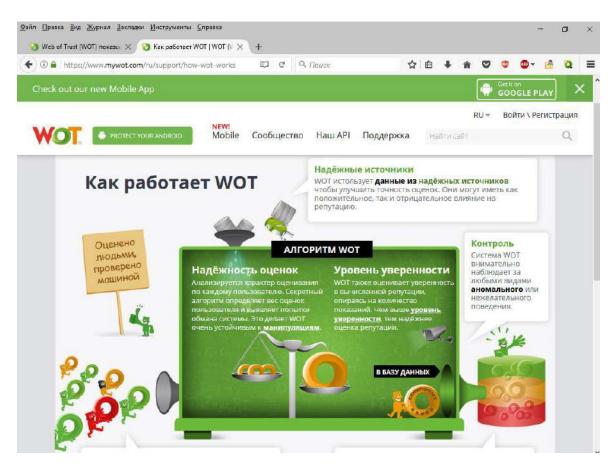
Предупреждение

Если вы попали на сайт с плохой репутацией по мнению пользователей, WOT покажет предупреждение.

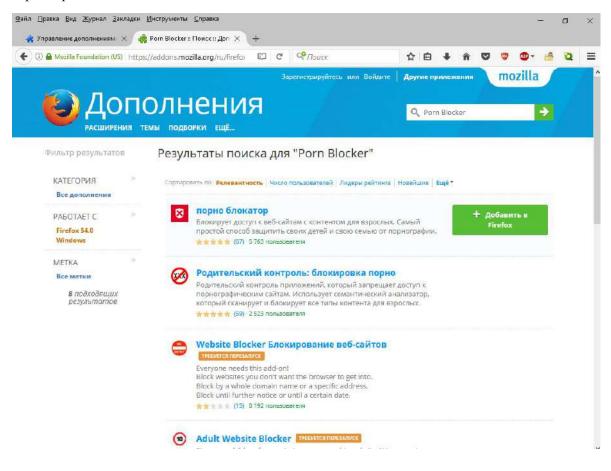
WOT предупреждает, но окончательное решение всегда за вами: вы можете проигнорировать предупреждение и зайть на сайт или вернуться на предыдущую страницу.



Если вы сами оцените сайт и поставите ему положительную оценку, WOT больше не будет показывать вам предупреждениє для этого сайта.

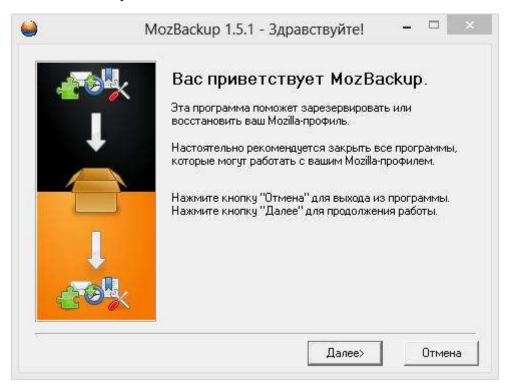


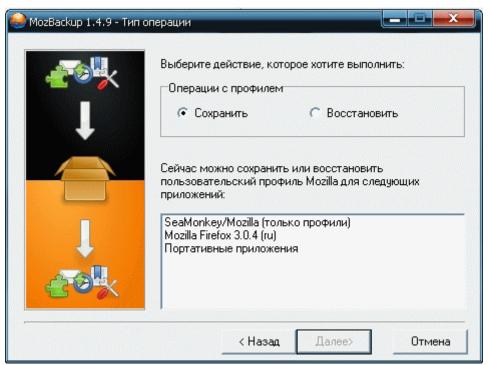
Есть и другие дополнения Firefox, блокирующие деструктивную информацию, как Porn Blocker и ему подобные, но следует иметь в виду, что далеко не все из них могут быть настраиваемы, а некоторые могут конфликтовать, и потому такие дополнения нужно устанавливать тестово на свой страх и риск.



Для того, чтобы сохранить профиль Firefox, используется утилита MozBackup, которую мы загружаем отсюда (http://mozutil.mozilla-russia.org/soft/MozBackup-ru.exe). После её стандартной установки (все параметры оставляем по умолчанию) закрываем браузер и открываем эту утилиту.

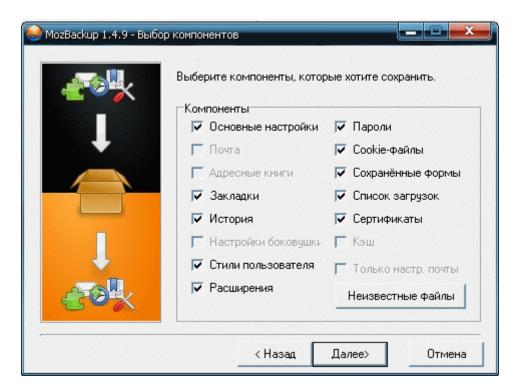
Пошагово действуем так:





После двух шагов выбираем профиль браузера и путь сохранения профиля (например, Рабочий стол ОС).

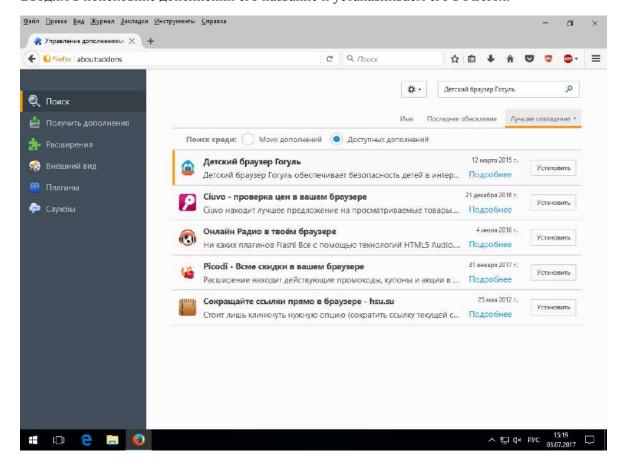
Далее галочками помечаем, какие данные браузера мы желаем сохранить и дожидаемся завершения операции.



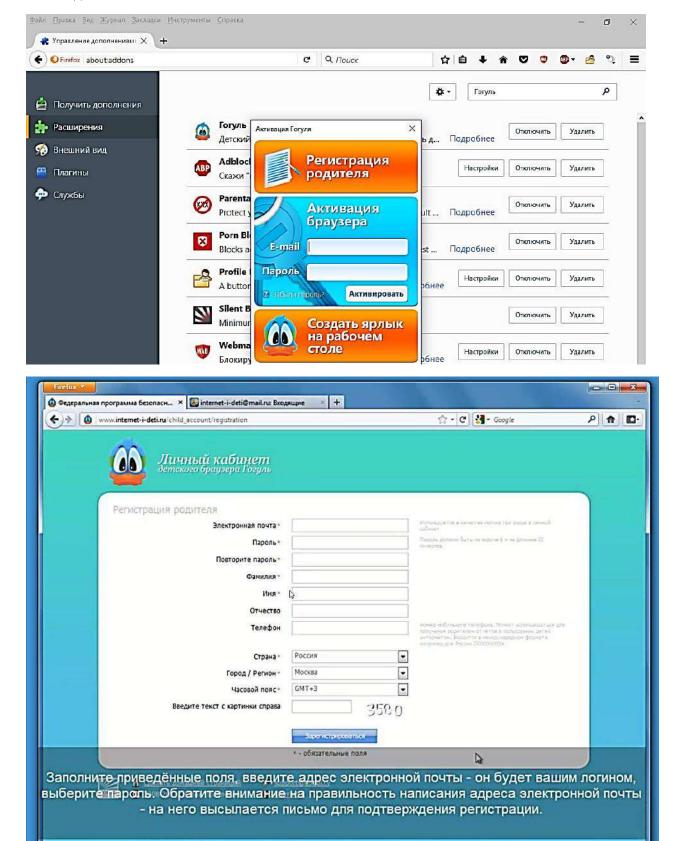
Шаг 4: Установка и настройка детского браузера «Гогуль»

Для детей необходим специальный браузер, который желательно должен быть установлен в отдельном Firefox на отдельном компьютере. На настоящий момент есть отечественная разработка – детский браузер «Гогуль».

Вводим в поисковике дополнений его название и устанавливаем его в Firefox.



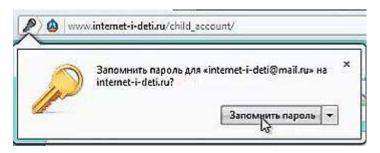
Установщик попросит перезапуска, что мы и сделаем. При клике на пункт меню «Инструменты»- «Гогуль» появится окно дополнения, из которого требуется пройти регистрацию учетной записи на сайте «Гогуль» (для регистрации используем учетную запись почтового ящика сервиса https://protonmail.com). В некоторых снимках инструкции приведены согласно обучающему видео с сайта дополнения.





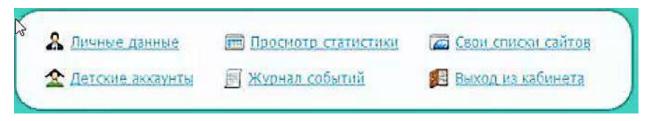


Тут выходим из учетной записи и заходим снова, введя адрес электронной почты и пароль. Появится всплывающее окно в левом углу с вопросом о запоминании пароля для сайта «Гогуль» - нажимаем «Запомнить пароль».





Меню сайта дополнения представляется таким. Заходим в пункт меню «Детские аккаунты».

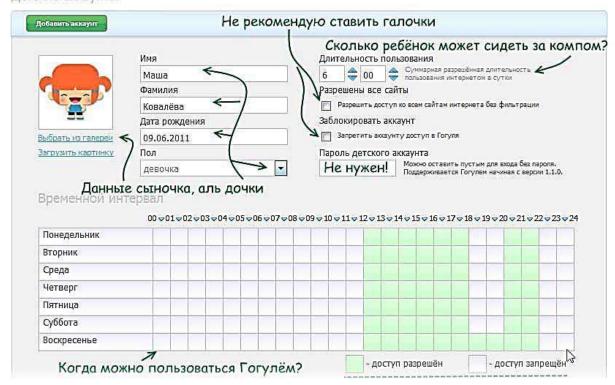




Нажмем кнопку «Добавить аккаунт». Далее введем учетные данные. Опционально можно задать пароль входа детской учетной записи, длительность и временной интервал (сверху указаны числа месяца, слева - дни недели) по дням пользования браузером.



Детские аккаунты



После добавления детской учетки в «Гогуль» потребуется определить свои списки сайтов.





Также можно добавить сайты из закладок, что хранятся в вашем браузере одною кнопкой «Импорт сайтов».

Нужно после установки Гогуля зайти в Mozilla Firefox в "инструменты" и в списке находим детский браузер! Щёлкаем левой клавишей по Гогулю!



Теперь, если у нас ярлыка нет на рабочем столе, то мы нажимаем "создать ярлык на рабочем столе".

Вводим свою почту и пароль (что указывали при регистрации родителя) и тычем "активировать".



Как мы видим, у нас есть аккаунт нашей детворы. "Нажимаем" на Машу и двигаемся дальше.

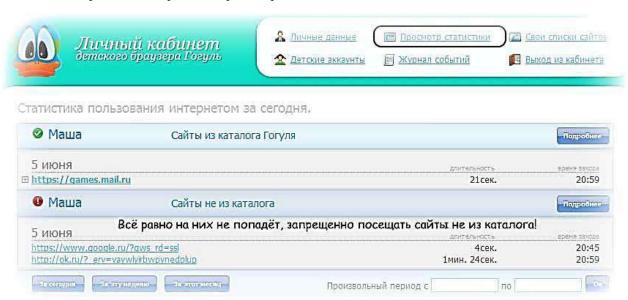


В чём суть?

У ребёнка будет детский браузер! Он не сможет зайти в Гугл или Яндекс! Только сайты, что одобрены психологами т.е. детские, грубо говоря, ваш ребёнок отныне защищён! Сразу бросается в глаза цветовой фон, вот бы и у взрослых было такое оформление!

Ваша задача – научить своего малыша, дать ему азы для путешествия по Гогулю! Так, расскажите ему про поиск и возвращение на главную т.е. на официальный сайт детского браузера.

У нас получилось! Однако, куда же заходил ребёнок? Для этого, мы входим в родительский кабинет и отправляемся в раздел "просмотр статистики".





Теперь необходимо ознакомиться с программой «Angry Duck», блокирующее доступ к приложениям. Загружаем отсюда: http://www.gogul.tv/download/angryduck/

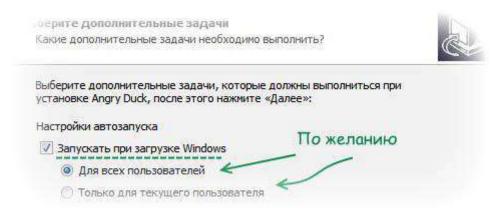


Сама установка банальна! Мы выбираем путь установки, можно оставить по умолчанию.



Запускать при загрузке Windows – галочку нужно ставить, если дитё уже умеет самостоятельно включать компьютер, в таком случае, программа начнёт функционировать с включением компьютера.

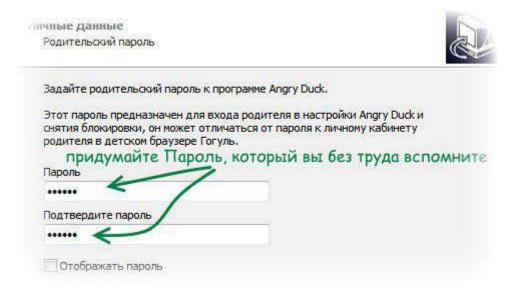
Рекомендую выбрать для всех пользователей, чтобы дитятко случайно не зашёл под другой учётной записью!



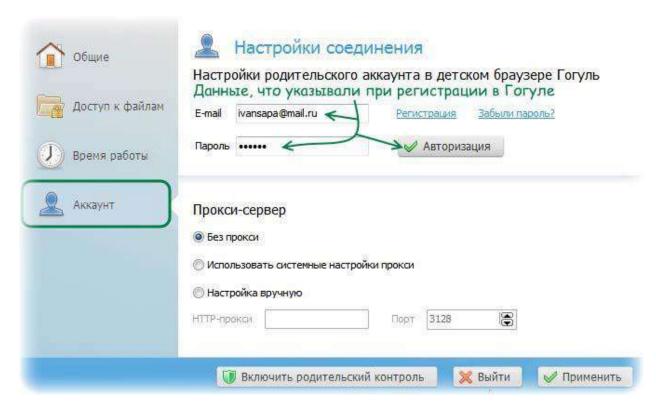
К паролю нужно отнестись внимательно, ибо вам без него потом не попасть в собственный браузер, а фишка ещё в том, даже если вы надумайте удалить Angry Duck с вас всё равно спросят этот пароль.

Посему, запишите его обязательно, а лучше ещё и запомните т.е. это должно быть нечто знаковое, что вы без труда вспомните в любое время года.

Кстати, пароль можно сделать исключительно из цифр: 7587 и тому подобное, экспериментируйте!



Вот мы установили и запустили Angry Duck, осталось лишь авторизоваться! Мы отправляемся во вкладку "аккаунт" и вводим электронный адрес и пароль, что указывали при регистрации в Гогуле.

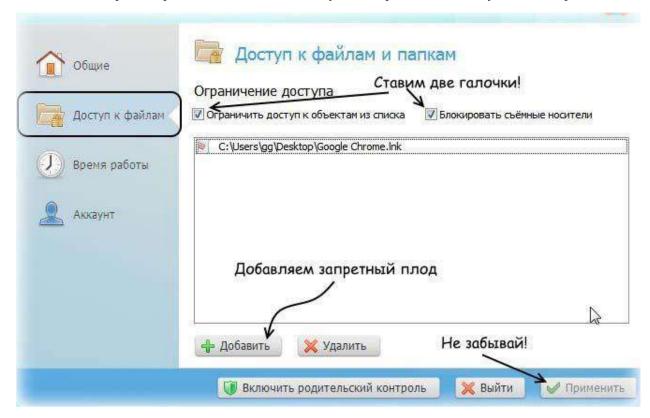


Изначально, ПО блокирует лишь браузеры (кроме Гогуля), следовательно, нам нужно заблокировать приложения, что будут вредны.

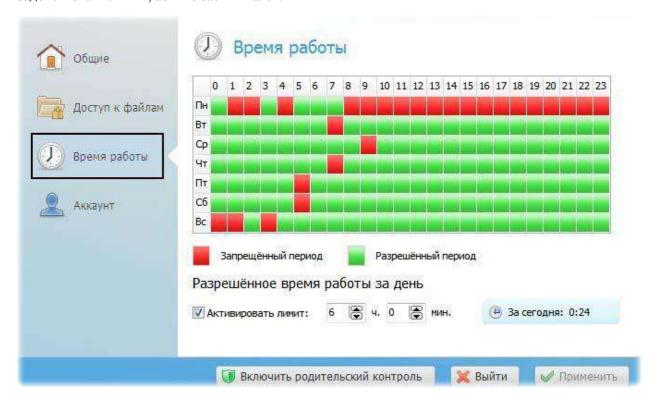
Просто, жмём "добавить" и находим вредную игрушку на своем компьютере.

Блокировать съёмные носители – это диски, флэшки и иные хранилища данных, что могут быть подсоединены к компьютеру через USB-вход или дисковод.

Можно заблокировать файл, но для надежности нужно запретить всю папку с данным файлом.



Мы также выбираем дни или часы, что будут запрещены для использования и ещё можем задействовать лимит, абы не засиживался.



Так, если ребёнок запустит компьютер в "запрещённый час", то он попросту не сможет ничего сделать, всплывёт окошко с предложением ввести пароль. Так что, главное не сообщать заветные циферки или буковки своему чаду.



Просто! Нажмите "включить родительский контроль", а также Angry Duck может запускаться при включении компьютера.

Запомните, что если вы введёте пароль, то защита спадёт! Соответственно, все запрещённые браузеры и программы станут доступны. Тут всё держится чисто на пароле, убрали его – блокировка пропала!



Проверить работоспособность можно с помощью трея (нижний правый угол рабочего стола). Там, рядом с часами будет утка — если она бледного цвета, значит, защита отключена, а если цветная (как на рисунке), то работает.

Общая осведомлённость заключается в функциях раздела "общие" в «Angry Duck».

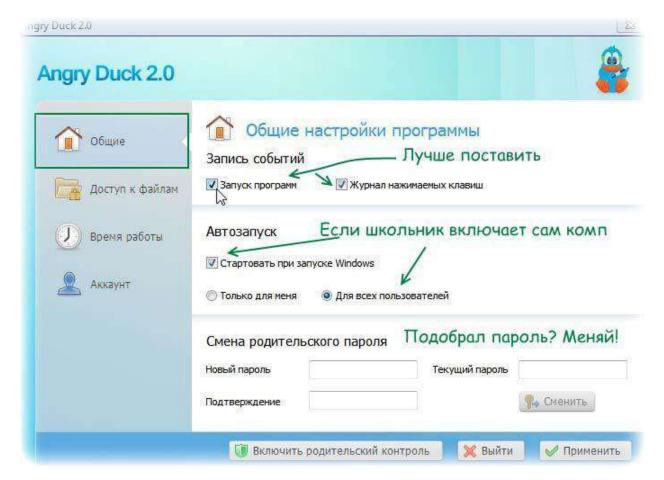
Запись событий – в какие программы лазил ваш ребёнок, пока вас не была дома? Что за кнопки он нажимал? Все сведения будут доступны в родительском кабинете. Галочки лучше поставить;



Автозапуск – одно дело, если малыш ещё толком не понимает происходящего. Другое дело, когда уже мальчику 7 или 8 лет, естественно, он сам включает компьютер и необъятный виртуальный мир поглощает его.

Однако, Angry Duck может начинать свою работу при запуске компьютера и, следовательно, запрещает посещать взрослые программы, рубиться в игрушки и проводить много времени за компьютером.

Смена родительского пароля – можете поменять на более запоминающийся или выбрать посложнее.



Но надо учесть, что не нужно использовать Гогуль в качестве запрета. Тем самым, ребёнок может подумать, что вы ему не доверяете!

А к чему это может привести?

К замкнутости, грубо говоря, вы потеряете связь с ребёнком, которую архисложно восстановить.

Детский браузер – это ограничительная мера, но ни в коем случае не запрещающая, уясните этот тонкий момент! Покажите ему всё богатство его нового сокровища, расскажите про детский мир, что доступен в интернете.

Конечно, вы можете добавить свои сайты в каталог Гогуля. Да к тому же с дополнением Angry Duck вы сможете не засиживаться подолгу перед экраном монитора.

Таким образом, детский браузер подходит как для маленьких, так и для взрослых!

Шаг 5: Использование DNS-фильтрации содержимого Интернет

Кроме браузера и дополнений есть ещё барьер с использованием DNS – компьютерной распределённой системы для получения информации об именной принадлежности сайтов. На ниже приведенном снимке показывается указание DNS-фильтрации при помощи поисковой службы «Яндекс» (адреса обведены красным), которая блокирует вывод результатов нежелательных запросов.

