Рекомендации о защите детей от информации, причиняющей вред здоровью и развитию

РЕКОМЕНДАЦИИ
ПО ЗАЩИТЕ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ, В ТОМ ЧИСЛЕ ОТ ПРОПАГАНДЫ НАСИЛИЯ, ЖЕСТОКОСТИ И ДРУГИХ СОЦИАЛЬНЫХ ДЕВИАЦИЙ В СМИ, ИНТЕРНЕТЕ И ДРУГИХ СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

Безопасность детей в социальных сетях. Родительский контроль.
Нынешние дети начинают учиться считать, писать и читать практически одновременно с работой за компьютером. Хорошо это или плохо — вопрос спорный. Но несомненно, что освоение компьютера с юных лет открывает широкие возможности в плане развития и образования, которые чаще всего реализуются при активном подключении родителей в качестве направляющей и контролирующей стороны.

В России около 8 миллионов пользователей глобальной сети — дети. Они могут играть, знакомиться, познавать мир… Но в отличие от взрослых, в виртуальном мире они не чувствуют опасности. Наша обязанность — защитить их от негативного контента.

ВИДЕО – опасности Интернета для детей:
http://www.youtube.com/watch?v=8AOhNqnTGok&feature=player_embedded
http://www.youtube.com/watch?v=Gj-NciF1Qx0&feature=player_embedded
http://www.youtube.com/watch?v=Z21mYVa-VmE&feature=player_embedded

Как правило, родителям требуется организовать контроль за временем работы на компьютере (время приходится ограничивать), регулировать доступ к «вредным» программам (в частности, к играм), а также наблюдать за использованием Интернета и блокировать доступ к неподходящим для ребенка ресурсам.

С 2004 года в первый вторник февраля празднуется Всемирный день безопасного Интернета. В условиях быстрых темпов развития информационных технологий необходимость контроля Интернета становится вопросом первостепенной важности. Рискам, таящимся в киберпространстве, особенно подвержены дети. Глобальная сеть ничуть не безопаснее игровой площадки. Это понимают во всем мире.

- Сегодня не нужно работать в ФСБ, чтобы узнать о человеке все, достаточно залезть в Интернет, и Вы найдете фамилию, возраст, адрес, место учебы, материальное положение. Практика показывает, что дети в поисках друзей размещают о себе в Сетях только голую правду. А опытным мошенникам не остается ничего кроме как воспользоваться их наивностью и недостатком родительского контроля. Преступники в Интернете действуют по принципу волка в овечьей шкуре. Они пользуются тем, что дети не могут распознать взрослого, умело маскирующегося под их сверстника. Только контролируя Интернет, отслеживая переписку ребенка, родители могут обнаружить тех, кто отправляет подозрительные сообщения их детям, пытается втереться к ним в доверие, договориться о встрече, задает наводящие вопросы и забрасывает просьбами выслать откровенные фотографии.
- Глобальная Сеть содержит большое количество информации взрослого содержания. Интернет насчитывает сотни миллионов порнографических страниц. Порнография считается одной из самых прибыльных отраслей. Эта индустрия в Интернете

приносит около 2,5 миллиардов долларов в год. А количество порнографических страниц с каждым годом растет в десятки раз быстрее, чем грибы после дождя.

- Другая серьезная проблема — распространение наркотиков через Глобальную Сеть. Достаточно набрать в поисковике название наркотического средства, чтобы узнать всё, начиная от того, как его приготовить до того, где взять. В апреле 2012 года Президент РФ Дмитрий Медведев на заседании президиума Государственного совета России выступил за контроль Интернета на предмет пропаганды наркотиков.
- В Интернете легко найти информацию суицидального характера, видеоматериалы по дракам, вскрытиям. Здесь же дети, оставшись без надлежащего контроля родителей, могут свободно познакомиться с любыми формами экстремизма.
- Интернет – реальный пожиратель времени. В поисках развлечений, играя или просто зависая в чате, можно проводить часы драгоценной жизни. В последние годы набирает обороты болезнь под названием «Интернет-зависимость». Дети начинают пропускать уроки, хуже учиться, становятся раздражительными. По мнению врачей, родителям следует контролировать, чтобы младший школьник проводил за компьютером не больше четверти часа. Бесконтрольное сидение в Интернете ведет к тому, что дети теряют зрение, перестают заниматься спортом, теряют навыки общения вне Сети. В Китае несколько подростков умерли за компьютером не в силах оторваться от экрана, чтобы поесть.
- Кроме того, через Интернет легко проникают вредоносные программы в виде вложенных файлов электронных писем, троянских коней, HTML и Java-вирусов и могут привести в поломке компьютера.

Вот почему идею празднования дня контроля Человека над Интернетом поддержали во всем мире. **С 2008 года в России существует Национальный узел Интернет-безопасности — Центр безопасного Интернета**. Он посвящен проблеме безопасной, корректной и комфортной работы в Глобальной сети. Создатели проекта уверены, что в условиях ускоренных темпов внедрения Интернета в повседневную жизнь граждан защита наших детей от рисков, скрытых в недрах всемирной паутины, требует активной позиции каждого.

Родительский контроль компьютера

Программы родительского контроля предназначены, в первую очередь, для создания ограничений ребенку, они призваны обеспечить его безопасность, оградить от того, что, возможно, ему еще рано знать и видеть. Одна из основных задач приложений – создание фильтра веб-сайтов. Все очень просто: на одни страницы заходить можно, на другие – нельзя. Как осуществляется подобный контроль? Обычно предлагается два варианта ограничений.

Приложение работает с базой данных, где содержатся сайты для взрослых. Крайне желательно, чтобы список регулярно обновлялся через Интернет, иначе появление новых ресурсов быстро сделает защиту неактуальной. Администратор или, в данном случае, родители могут расширять черный список сайтов на свое усмотрение.

Довольно часто применяется более жесткий способ контроля – создание белого списка. Ребенок может посещать только те веб-сайты, которые ему разрешили родители. Минус подобного контроля заключается в чрезмерной строгости, можно даже сказать, в жестокости. Пустили дочь за компьютер, а сайт с описаниями технических характеристик кукол не включили в белый список. Девочка в слезах. Подружки давно хвастаются новинками кукольного мира, а ребенок даже не в курсе, о чем вообще сверстники ведут разговор, Интернета-то нормального нет. Зато не надо автоматически обновлять списки, актуальность со временем практически не теряется.

Еще один способ родительского контроля заключается в фильтрации сайтов по их содержимому. Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на веб-странице, то она не открывается. Родителям, возможно, придется отбросить прочь страх и стыд, самостоятельно вписывая мат, пошлости, уголовщину и прочие вещи, запрещенные для ребенка.

Обеспечение безопасности ребенка за компьютером заключается не только в ограничении доступа к веб-сайтам. Есть еще одна, если так можно выразиться, группа риска – это программы обмена мгновенными сообщениями. Ребенок наивен, он можно нечаянно рассказать незнакомцу ваши личные данные. Злоумышленники хитры, они прикидываются ровесниками, невзначай задают каверзные вопросы. Напрашивается и вторая опасность – собеседники ребенка могут научить его, в лучшем случае, мелким пакостям, а о примерах серьезных бед лучше даже не вспоминать. Некоторые программы родительского контроля способны производить анализ информации, отправляемой с компьютера. Если в ней встречаются некие ключевые слова, например, адрес, номер школы или телефона, то происходит блокировка отправки сообщения.

В вашей семье один ребенок или несколько детей, есть компьютер, подключенный к Интернету. Как обезопасить младшее поколение от негативных последствий пребывания в Сети? Первое, что сразу напрашивается – компьютер не должен стоять в детской комнате. Лучше всего, если он будет в зале, где кто-нибудь родителей сможет постоянно следить за тем, чем занимается ребенок. В противном случае, он запрется в комнате, и вы даже, возможно, не догадаетесь, что чадом скачано несколько фильмов эротического содержания, а в местном чате ему рассказали, как самому делать петарды.

Ребенку надо показать Интернет, заинтересовать полезными, с вашей точки зрения, сайтами, объяснить, что можно делать, а что нельзя. Нельзя соглашаться на встречи с незнакомыми людьми, нельзя сообщать личные данные, нельзя самостоятельно совершать покупки в сетевых магазинах. Ну а вместо нравоучений сыну «не смотри на голых женщин», уместней воспользоваться специальными программными продуктами, которые закроют ему доступ к взрослым ресурсам.

Родительский контроль компьютера — это набор программ и действий, который направлен на организацию или запрет использования детьми компьютерного времени, доступа к играм или другим программам, и самое главное — для избежания просмотра сайтов с “недетским” содержимым.
Функция родительского контроля недоступна, если компьютер подключен к домену.

В Windows 7 можно устанавливать ограничения на использование детьми компьютера и повысить их безопасность в Интернете, не контролируя каждое их действие лично.

Функция родительского контроля позволяет ограничивать часы работы детей на компьютере, а также устанавливать перечень доступных им программ и компьютерных игр (и время их использования). Кроме того, с помощью родительского контроля в составе Windows Media Center можно блокировать доступ к просмотру нежелательных телепередач и фильмов.
Чтобы повысить безопасность детей в Интернете, загрузите Семейную безопасность Windows Live. Эта бесплатная программа поможет вам управлять списком веб-сайтов, которые доступны вашим детям, и контактов, с которыми они могут общаться по сети. Она также предоставляет полезные и простые в изучении отчеты об их действиях в Интернете.

Несложно просмотреть, чем занимался ребёнок в интернете в Ваше отсутствие. Простые примеры: после настройки родительского контроля компьютер сына или дочки будет включаться только после 6 вечера; игры будут доступны до 10 часов ночи; ни один сайт, содержащий в названии набор букв (s)*ex или por*(n), не будет открываться.

Идеального рецепта настройки родительского контроля не существует, поскольку тут всё зависит от целого ряда факторов: уровня компьютерной подготовки ребенка и его родителей, компьютерных предпочтений и степени сознательности подрастающего поколения и, наконец, от отношения самих родителей к данной проблеме. Вариантов организации родительского контроля несколько. Можно ограничиться встроенными средствами Windows, задействовать модули родительского контроля в решениях класса Internet Security, подключиться к сервисам для фильтрации нежелательных сайтов либо установить специализированные программы родительского контроля.

Родительский контроль скачать бесплатно вполне возможно, существуют хорошие некоммерческие программы, и зачастую многим пользователям достаточно уже встроенных в Windows инструментов.

Встроенный в Windows 7 родительский контроль
Встроенные средства Windows 7/Vista позволяют вводить некоторые ограничения, касающиеся работы ребенка на компьютере, — устанавливать временной интервал, в течение которого дети могут пользоваться компьютером, а также определять перечень доступных игр и приложений. Этого может оказаться вполне достаточно для ограничения компьютерной деятельности детей младшего возраста.

В Windows Vista дополнительно предусмотрен функционал для блокирования доступа к некоторым сайтам и другим интернет-сервисам. Операционная система Windows 7 встроенного вебфильтра не имеет — по замыслу разработчиков для организации расширенного родительского контроля в этой ОС предназначена программа Family Safety («Семейная безопасность») из пакета Windows Live Essentials 2011. С ее помощью можно блокировать доступ к нежелательным сайтам, определять контакты, с которыми ребенок может общаться через Интернет (только в Windows Live Hotmail и Windows Live Messenger), и просматривать отчеты о действиях чада в Сети.

Для настройки родительского контроля встроенными средствами Windows необходимо иметь отдельную учетную запись с правами администратора, а также одну (или более, если детей несколько и требуется разграничение прав) учетную запись обычного пользователя, под которой ребенок будет заходить в систему. Разумеется, гостевой профиль должен быть отключен, а на профиль администратора установлен пароль — в противном случае ребенок рано или поздно отключит родительский контроль и будет использовать компьютер безо всяких ограничений.

Технология настройки ограничений никаких сложностей не вызывает — достаточно из панели управления открыть модуль «Родительский контроль», выбрать учетную запись, под которой заходит ребенок, и определить требуемые настройки.

Можно, например, настроить расписание работы по дням недели, что позволит ограничить общее время работы на компьютере, поскольку по окончании разрешенного периода времени будет происходить автоматический выход из системы. Не сложнее окажется отрегулировать доступ к играм, установив на них общий запрет, либо запретив доступ только к отдельным установленным на компьютере играм, указав их вручную либо путем выбора возрастной категории.

Стоит отметить, что полный запрет на игры — вполне разумная (а вовсе не драконовская) мера, которая имеет смысл, если у ребенка для работы на компьютере используются два профиля: «Ученик» и «Игрок». При этом для профиля «Ученик» полностью запрещен доступ к играм, а для профиля «Игрок» установлены четкие временные рамки, что позволяет ограничить время на компьютерные игры, но разрешить доступ к компьютеру в учебных целях. В дополнение также стоит отметить, что ограничение доступа по времени легко может быть обойдено путем смены компьютерного времени, о чем рано или поздно догадается любой ребенок. Поэтому установка пароля на BIOS — условие обязательное, которое для надежности также может быть подкреплено настройкой синхронизации времени на компьютере с временны*ы*ми серверами в Интернете.
Однако, пункт Игры в Родительском контроле Windows 7 кажется полезным только сначала. Во-первых, здесь могут быть представлены не все игры, установленные на компьютере. Во-вторых, лучше настроить эти ограничения в Разрешении и блокировке конкретных программ.

В этом пункте перечислены все установленные на компьютере программы (вернее, Windows считает, что все). Здесь можно запретить или разрешить каждое из приложений, однако помните: этот список может быть неполным. Лучше поискать вредные программы самостоятельно (кнопка Обзор), и заблокировать их. И не забудьте в конце выключить Гостевой профиль пользователя — на него не распространяются никакие ограничения!

Другие программы для родительского контроля
Более продвинутые программы во многом имеют похожие функции с разными названиями. В них несложно разобраться за несколько минут, и почти в каждой из них на вопрос как установить родительский контроль отвечает пошаговый мастер настроек — он запускается при первом использовании программы.

В декабре 2012 года порталом Anti-Malware.ru было проведено тестирование модулей Родительского контроля в ведущих программных решениях производителей по обеспечению безопасной работы в сети Интернет. В результате тестов были определены 4 программных продукта, которые наиболее эффективно ограничивают просмотр детьми нежелательного контента — KinderGate Parental Control 1.5, Kaspersky Internet Security 2013, ContentKeeper Express и Avira Internet Security.

1. Рекомендуем вначале обратить внимание на проект SkyDNS (www.skydns.ru) — это не программа, а целый щит, ограждающий ваш компьютер от потенциально опасных сайтов.

Разработчик: Айдеко

Сайт сервиса: https://www.skydns.ru/

Работа под управлением: Windows, Mac OS X, Linux

Цена: «Премиум» — 295 руб. в год; «Школа» — 4500 руб. в год; «Бизнес» — 300 руб. в месяц

Зарегистрировавшись на сайте проекта, вы получаете гораздо более безопасный сёрфинг интернета. Проект заносит в свой чёрный список сайты с сомнительным содержимым, предоставляя свободный доступ к остальным, “правильным” ресурсам. Проект постоянно обновляется, и ложных срабатываний почти не случается. SkyDNS — бесплатный ресурс, который отсечёт сразу половину проблем с доступом на нежелательные сайты. Сервис родительского контроля SkyDNS позволяет делать множество вещей даже для школ.

SkyDNS — «облачный» российский сервис интернет-фильтрации на уровне DNS-запросов, который обеспечивает блокирование опасных и нежелательных для просмотра детьми сайтов. Данный сервис был запущен в 2010 году и в настоящее время работает в нескольких режимах — бесплатном Free (с ограниченным функционалом) и трех коммерческих: «Премиум», «Школа» и «Бизнес». Для настройки блокирования сайтов, нежелательных для просмотра детьми, предназначены тарифы «Премиум» и «Школа». Тариф «Премиум» рассчитан на применение всеми пользователями семьи (позволяет защитить сразу несколько компьютеров) и может работать в специальном «детском» режиме. Тариф «Школа» ориентирован на использование в учебных заведениях и не имеет ограничений на число защищаемых компьютеров. Возможности обоих тарифных планов обеспечивают блокирование разнообразных нежелательных ресурсов (содержащих порнографию, рекламу наркотиков, пропаганду расовой ненависти, агрессии и пр.), а также позволяют защитить компьютер от сайтов, замеченных в распространении вирусов и фишинге, ограничить доступ к социальным сетям, форумам и др.

Настройка защиты компьютера через сервис SkyDNS не совсем очевидна, хотя и занимает в целом немного времени. На первом этапе нужно зарегистрироваться на сервисе, войти на сайт SkyDNS под своим аккаунтом, перейти на вкладку «Фильтр» и указать категории, которые необходимо заблокировать. После этого можно дополнительно отрегулировать доступ на уровне отдельных сайтов (то есть с обходом настроек общего фильтра) на вкладке «Исключения». В принципе сервис может работать и без регистрации, но в анонимном режиме обеспечивается только фильтрация от сайтов, распространяющих вирусы, а также от фишинговых ресурсов. Стоит отметить, что в платных тарифах предусмотрено использование профилей фильтрации, позволяющих устанавливать разные правила фильтрации в рамках одного аккаунта (например, для детей и взрослых). Определение блокируемых категорий через сервис SkyDNS:

Настройка белого и черного списков сайтов в SkyDNS:

Затем нужно настроить сетевое подключение компьютера или модема на работу со SkyDNS. Конкретные действия на этом шаге зависят от типа IP-адреса (статический или динамический). В случае статического адреса требуется указать в сетевых настройках DNS-адрес сервиса и привязать свой IP-адрес к своему аккаунту через вебинтерфейс.

Пользователям динамических IP-адресов нужно скачать и установить дополнительное приложение (например, в Windows утилиты SkyDNS Agent 2) с авторизацией. Данное

приложение отвечает за настройку сетевого подключения на работу со SkyDNS и обновление записи об IP-адресе пользователя. После этого доступ будет обеспечиваться только к разрешенным ресурсам. В ходе работы для каждого аккаунта ведется статистика посещений с отображением наиболее посещаемых сайтов, а также заблокированных ресурсов и категорий.

2. Среди классических вариантов родительского контроля последнее время наибольшей популярностью на компьютерах российских пользователей пользуется продукт, поставляемый в составе продуктов Лаборатории Касперского — Kaspersky Crystal и Kaspersky Internet Security. Отдельно установить «Касперский родительский контроль», к сожалению, не получится.

Сайт программы: **http://www.kaspersky.ru/kaspersky_internet_security**
Размер дистрибутива: 149 Мбайт

Работа под управлением: Windows XP/Vista/7

Цена: лицензия на два компьютера сроком на 1 год — 1600 руб.

Kaspersky Internet Security 2012 — ориентированный на домашних пользователей инструмент для многоуровневой защиты от всех интернет-угроз: вирусов, хакерских атак и спама. Данное решение базируется на параллельном использовании «облачных» и традиционных антивирусных технологий, что позволяет достичь максимального уровня безопасности компьютера. Продукт включает базовые инструменты обеспечения антивирусной безопасности, а также большой набор дополнительных модулей. В их числе — безопасная среда запуска приложений и браузеров, монитор активности программ, сетевой экран, родительский контроль и т.д.

Входящий в состав продукта модуль «Родительский контроль» позволяет регулировать доступ детей к вебсайтам и их общение в социальных сетях («ВКонтакте», «Одноклассники.ру», Facebook, Twitter и др.) и через программы обмена сообщениями (ICQ и др.), а также ограничивать время доступа к компьютеру и отдельным приложениям. Главное окно Kaspersky Internet Security:

Настроить родительский контроль в Kaspersky Internet Security очень просто. Достаточно в окне модуля «Родительский контроль» выбрать учетную запись ребенка и отрегулировать настройки. Таким способом можно ограничить время работы ребенка на компьютере либо в Сети, составив расписание и/или ограничив отводимое на это суммарное время в сутки, а также определить разрешенные/запрещенные для использования приложения (в том числе по времени).

Определение расписания для пребывания в Интернете в Kaspersky Internet Security:

Несложно ввести ограничения на доступ к вебсайтам в зависимости от их содержимого. Настраивается система ограничений путем выбора категорий вебсайтов, доступ к которым следует заблокировать, формирования списка исключений (при необходимости) и включения/отключения режима безопасного поиска, который будет применяться во время работы пользователя с поисковыми системами (для Google и Bing.com). Настройка контроля посещения веб-сайтов в Kaspersky Internet Security:

Кроме того, разрешается ограничивать загрузку определенных типов файлов и осуществлять контроль переписки через интернет-пейджеры и в социальных сетях путем

блокирования переписки с контактами, с которыми общение запрещено. Предусмотрен мониторинг переписки с учетом употребления указанных родителем конкретных слов и блокирование пересылки данных, содержащих персональную информацию (например, домашний адрес, номер телефона). Все действия пользователей, для которых настроен родительский контроль, фиксируются в детальных отчетах по всем категориям контролируемых событий

3. ContentKeeper Home — «облачная» система фильтрации веб-контента, которая ориентирована на домашних пользователей.

Сайт сервиса: https://home.contentkeeper.com/
Работа под управлением: Windows 2000/XP/Server 2003/Server 2008/Vista/ 7

Цена: 29,95 долл.

Система обеспечивает очень высокое качество фильтрации при минимальной нагрузке на ресурсы компьютера, что является результатом применения технологии SaaS (Software as a Service), в которой основная функциональность выполняется в «облаке» на специальных серверах ContentKeeper. Система фильтрации ContentKeeper Home предлагается на коммерческой основе, для ознакомления доступна бесплатная лицензия сроком на один месяц. Данное решение позволяет родителям легко отслеживать, управлять, контролировать и обеспечивать безопасность работы в Интернете для всех членов семьи. Контроль осуществляется путем блокирования доступа к неподходящему или вредному контенту и ресурсам, содержащим ключевые слова из списка ключевых слов, ограничения доступа к программам чатов (Google Talk, MSN Messenger, Yahoo Messenger и др.) и к определенным типам файлов (аудио и видеофайлы, приложения и пр.). К сожалению, популярные в России программы чатов (ICQ, Miranda, QIP) не поддерживаются, зато список доступных для блокирования типов файлов внушителен.

Администрирование ContentKeeper Home осуществляется через вебинтерфейс и может производиться локально либо в удаленном режиме. Для настройки параметров фильтрации необходимо зайти на сервис, зарегистрироваться в панели управления под своей учетной записью и установить ограничения. Настройка производится для каждой из имеющихся учетных записей по отдельности, а это значит, что для детей и родителей могут быть определены разные политики доступа. Самый быстрый способ установить ограничения по конкретной учетной записи — выбрать один из предустановленных профилей настроек Предусмотрена также возможность создания пользовательских наборов фильтров, что позволяет решать конкретные задачи ограничения доступа. Готовых профилей доступа четыре:

- Education Only — работа только с образовательными ресурсами;
- No Facebook Or MySpace — блокирование доступа к социальным сетям;
- Block All Access — полное блокирование доступа в Интернет;
- Default — блокирование сайтов с порнографией, азартными играми и ресурсов, связанных с наркотиками.

Управление доступом в ContentKeeper Home:

Выбор для учетной записи предустановленного профиля в ContentKeeper Home:

Конфигурация любого из предустановленных профилей может быть изменена. Например, несложно открыть или закрыть доступ к ресурсам конкретных категорий, определить режим работы для программ чатов (запретить, разрешить или разрешить с ведением

отчета о сообщениях) и установить для конкретных поисковых систем режим безопасного поиска (Yandex.ru, Rambler.ru и Mail.ru не включены). Можно также создать белый и черный списки ресурсов, включить или отключить блокировку сайтов по ключевым словам и разрешить либо запретить загрузку определенных типов файлов.

Корректировка параметров профиля Education Only в ContentKeeper Home:

Кроме того, имеется функционал для настройки расписания доступа к Сети, правда здесь используется 12-часовая система времени (в сутках два интервала — «до полудня» и «после полудня») и неделя начинается с воскресенья, что непривычно для россиян, а потому большинству пользователей он может показаться неудобным. Реализован мониторинг использования Интернета с формированием отчетов по просмотренным категориям и наиболее посещаемым ресурсам, причем получить доступ к отчетной информации можно с любого компьютера в реальном времени.

4. Time Boss — простая и удобная программа для организации родительского контроля. С ее помощью родители легко могут ограничивать время компьютерной деятельности ребенка (в том числе в играх и Интернете), определять перечень доступных приложений (включая игры), вводить ограничения на ряд системных операций, запрещать доступ к отдельным папкам, а также регулировать посещение сайтов при интернет-серфинге.

Разработчик: Nicekit Software

Сайт программы: **http://nicekit.ru/parental-control/time-boss.php**
Размер дистрибутива: 1,8 Мбайт

Работа под управлением: Windows XP/Vista/7

Цена: Time Boss — 600 руб.; Time Boss PRO — 800 руб.

Программа обеспечивает контроль для всех зарегистрированных в системе пользователей и потому при необходимости может быть использована для настройки разных вариантов ограничений по различным профилям. В целях защиты от взлома подрастающим поколением разработчики предусмотрели ряд возможностей: использование пароля доступа к программе, работу в скрытом («Стелс») режиме, защиту от удаления приложения при загрузке Windows в безопасном режиме Safe mode и др. Приложение предлагается в двух редакциях: базовой Time Boss и расширенной Time Boss PRO. Редакция Time Boss PRO дополнительно предоставляет функционал для удаленного управления в рамках локальной домашней сети (можно удаленно менять настройки, оперативно добавлять время и пр.) и оснащена защитой от кейлоггеров (чтобы исключить возможность получения ребенком пароля доступа к программе).

Принцип использования Time Boss очень прост — для каждого пользователя Windows создаются профили типов «Родитель» и «Ребенок». Пользователям типа «Ребенок» настраивается компьютерное расписание, которое позволит четко определить часы для работы на компьютере в целом, а также в Интернете и с конкретными приложениями путем управления белыми и черными списками. Последнее окажется полезным для

ограничения игровой деятельности — игры можно вовсе запретить, указав их в черном списке, либо разрешить только по вечерам — то есть после подготовки домашних заданий. В ходе настройки расписания разрешается не только устанавливать временны*е* интервалы, но и указывать общее допустимое количество компьютерного времени на день, а также вводить при работе принудительные перерывы При необходимости также можно вводить системные ограничения, например отключить панель управления и заблокировать запуск системного реестра, запретить изменение даты и времени, отключить модуль «Установка и удаление программ», сделать невидимыми отдельные диски, защитить от изменений папки и др.

Настройка системных ограничений в Time Boss:

При желании можно попытаться предотвратить посещение ребенком нежелательных сайтов при интернет-серфинге. Правда, возможности тут ограничены блокированием по ключевым словам (задействованы ключевые слова для базовых категорий) и с учетом черного и белого списков), что, впрочем, не мешает ограничить ребенку посещение социальных сетей (например, указав для ресурса *.vkontakte.ru максимальный лимит допустимого времени) и пр. К сожалению, интернет-фильтр работает только с IE, запуск других браузеров необходимо отключить.

Что касается мониторинга компьютерной деятельности, то родители без труда смогут узнать, чем занималось их чадо на компьютере, — в Time Boss ведется журнал учета работы пользователей, в котором фиксируются все имевшие место события, с определенной регулярностью делаются снимки экрана и сохраняется подробная статистика времени работы каждого пользователя.

Установка ограничений для работы в Сети (Time Boss):

5. Программа «KinderGate Родительский Контроль» — инструмент для организации контроля доступа детей в Интернет, рассчитанный на домашних пользователей и образовательные учреждения.

Разработчик: Entensys Corporation

Сайт программы: **http://www.kindergate.ru/**
Размер дистрибутива: 33,7 Мбайт

Работа под управлением: Windows XP/Vista/7

Цена: подписка на два месяца — 100 руб.; подписка на год — 490 руб.

Данное решение позволяет блокировать нежелательный контент (поддерживается URL-фильтрация по черным или белым спискам и фильтрация по категориям), вредоносные сайты, а также прокси-серверы и сайты анонимайзеры, через которые можно было бы

обойти подобную блокировку. В целях защиты от взлома юными хакерами предусмотрено обязательное использование пароля для доступа к программе. Решение включает функционал для мониторинга действий ребенка в Сети: отслеживание посещаемых ресурсов при серфинге, мониторинг сообщений в сетевых мессенджерах (поддерживаются протоколы ICQ, Jabber, MSN, Mail.ru, YMSG) и наблюдение за перепиской ребенка в социальных сетях «ВКонтакте», «Одноклассники» и Facebook. Кроме того, предусмотрен инструментарий для запрета загрузки разных видов контента (видео, аудио, изображения и пр.), настройки расписания доступа в Интернет и блокировки контекстной рекламы и баннеров.

В техническом плане использование программы «KinderGate Родительский Контроль» сложностей не вызывает. Предполагается, что домашний компьютер, на который собираются устанавливать это решение, используется преимущественно ребенком; при необходимости работы родителей систему контроля временно отключают путем запуска окна программы (естественно, требуется знание пароля). Для настройки ограничений необходимо сделать простые настройки. Например, для настройки фильтрации сайтов по их содержимому достаточно активировать вкладку «Запрет категорий» и перетащить бегунок на нужный уровень блокирования. Столь же несложно ввести запрет на загрузку определенного типа файлов и конкретных ресурсов, а также настроить режим доступа в Интернет по времени или календарю. Допускается использование и более сложных правил фильтрации — скажем, можно запретить категорию «Веб-почта», но разрешить доступ к ресурсу mail.yandex.ru в качестве исключения. При необходимости можно включить функцию «Безопасный поиск» (позволяет заблокировать запросы сомнительного характера в поисковых системах Яндекс, Google и др.) и режим морфологического анализа ресурсов (обеспечивает блокирование вебстраниц с запрещенными словами), а также настроить запись мгновенных сообщений. Вся деятельность ребенка в Интернете фиксируется в логах и отображается в виде отчетов (посещаемые ресурсы, трафик, заблокированные сайты).

Ограничение доступа к сайтам в программе «KinderGate Родительский Контроль»:

Блокирование загрузки контента («KinderGate Родительский Контроль»):

В дополнение можно посмотреть и другие программные продукты: КиберМама, KidsControl, Spector Pro, ParentalControl Bar.

!!! Но помните: ни одно программное обеспечение не идеально.
Даже после настройки компьютерных ограничений «на всё и вся» не стоит обольщаться — наложение запретов лишь активизирует многих юных компьютерщиков на поиски путей их обхода. Большинство подобных вариантов обхода может быть предусмотрительно заблокировано соответствующими системными запретами или настройками родительского контроля.

Существует множество методов обхода родительского контроля, и зачастую дети здесь более изобретательны и продвинуты, чем родители. Если программы родительского контроля расположены на домашнем компьютере (точнее, в его операционной системе),

то не слишком сложный метод избежания контроля — создание так называемого Live CD – загрузочного диска, который использует не основную ОС, а сам представляет из себя работоспособную «операционку» с настройками без ограничений доступа к интернету. Контрмеры существуют и для этого решения (заблокировать старт компьютера с компакт-дисков и запаролить BIOS), но если ребёнок смог создать CD-дистрибутив, то и здесь он вполне сможет справиться.

Как снять родительский контроль другими методами? Пятиминутная настройка любимого браузера или мессенджера с использованием прокси-серверов. Вкратце: большинство программ для интернета имеют специальные настройки, где можно задать использование для запросов внешних прокси-серверов. При этом домашний компьютер отсылает запрос на другой компьютер (прокси-сервер). Родительский контроль молчит: этот прокси не относится к списку запрещённых ресурсов. Внешний сервер обрабатывает запрос и выдаёт на экран требуемую информацию, где вполне может находиться запрещённое содержимое.

Зачастую дети всё равно получают доступ к запретному плоду. Всегда найдутся друзья, чей компьютер работает без родительского контроля. Всё большую популярность даже среди школьников набирают смартфоны и планшеты, которые контролировать ещё сложнее, чем компьютер. Всегда можно задать вопрос поисковику: родительский контроль как отключить, а методов снятия ограничений существует множество.

Скачать родительский контроль, установить и настроить его недостаточно: ни одна лучшая программа родительского контроля не даст гарантий от опасности. **В дополнение к программам нужен и визуальный доступ к компьютеру.** Очень рекомендуем устанавливать домашний компьютер в то место, где он находится на всеобщем обозрении. Не переборщите: нельзя открыто шпионить за ребёнком, просто поглядывайте время от времени на происходящее на мониторе. Да и подросток вряд ли захочет посещать неподходящие сайты, если знает, что родители могут легко это заметить.
Возможно, лучший метод родительского контроля в том, чтобы совместно обсудить опасности сомнительных сайтов? В дружеской и равноправной беседе родителей с детьми можно достичь согласия и понимания гораздо проще и результативнее, чем используя отключаемые программы и другие электронные методы. Запретный плод сладок.

Станьте друзьями для своих детей: старшими, мудрыми и опытными, с которыми хочется поговорить на любую тему с удовольствием. Это и есть самый лучший метод родительского контроля, который принесёт множество позитива в общение с детьми.

Помните об интернет-мошенниках
Согласно данным Федеральной торговой комиссии США, 31 процент жертв похищения личных данных составляют молодежь. Подростки становятся привлекательными объектами для мошенников, поскольку у них хорошие кредитные оценки и малый долг, по сравнению со взрослыми они меньше заботятся о безопасном хранении информации.

Некоторые моменты, о которых должны знать ваши дети, чтобы стать разумными потребителями и избежать интернет-мошенничества.

- **Никогда не разглашайте личную информацию.** Никогда не указывайте свою личную информацию, например полное имя или город проживания во время общения с помощью мгновенных сообщений или в чатах, если вы полностью не уверены в личности человека, с которым вы общаетесь.
- **Обязательно завершайте сеанс с выходом из системы при работе на общедоступном компьютере.** Если вы используете компьютер в библиотеке или в интернет-кафе, прежде чем покинуть компьютер, полностью завершите все сеансы с выходом из системы. Вы не знаете, какое программное обеспечение установлено на этих компьютерах, а также что оно выполняет. Кроме того, может быть установлено программное обеспечение, фиксирующее нажатие клавиш.
- **Придумывайте безопасные пароли и держите их в секрете.**
- **Используйте только безопасные сайты.** Если ваши дети совершают покупки в Интернете, то им следует каждый раз убеждаться в том, что URL-адрес сайта, на котором они вводят финансовую информацию, начинается с префикса https://, в правом нижнем углу имеется желтый значок замка или адресная строка отображается зеленым цветом. Они могут щелкнуть по значку замка или в адресной строке, чтобы проверить сертификат безопасности данного сайта.
- **Распознавание мошенников и сообщение о фактах мошенничества.**Расскажите своим детям о признаках подделки идентификационных данных: предложение утвержденных кредитных карт, звонки из агентств по сбору информации или незнакомые финансовые документы. Если у вашего ребенка возникнет подозрение на подделку личных данных, немедленно предпримите соответствующие действия, чтобы ограничить ущерб. Обратитесь в свою кредитную компанию, банки или все три организации по кредитной отчетности, а также в полицию. Закройте все счета, которые подвергались фальсификации, и попросите детей поменять пароли для всех своих учетных записей в Интернете. Ведите журнал всех выполняемых действий.

Указания для детей различных возрастов по использованию Интернета
!!! Очень важно помнить, что это только указания. Вы лучше знаете своих детей.
Для детей и их неравнодушных родителей существует бесплатная линия помощи «Дети онл@йн» http://detionline.com
Если ребенка оскорбляют и преследуют в интернете или ребенок стал жертвой сетевых мошенников, столкнулся с опасностью во время пользования сетью Интернет, если вы обеспокоены безопасностью ребенка при его работе в интернете, обратитесь на бесплатную линию помощи «Дети онл@йн». Эксперты помогут решить проблему, а также проконсультируют по вопросу безопасного использования детьми мобильной связи и интернет. Консультации проводят психологи и технические специалисты МГУ имени М.В. Ломоносова, Федерального института развития образования МОН РФ и МГТУ им. Баумана.

До 10 лет
Контролируйте своих детей, пока они не достигнут 10-летнего возраста. Можно использовать средства интернет-безопасности, чтобы ограничить доступ к содержимому, веб-сайтам и действиям, а также принимать активное участие в действиях ребенка в Интернете, однако рекомендуется всегда сидеть рядом с детьми, когда они используют Интернет, пока они не достигнут 10-летнего возраста.

Советы по безопасности при использовании Интернета вместе с ребенком **в возрасте от 2 до 10 лет:**

1. Никогда не рано начинать формировать открытое и позитивное общение с детьми. Желательно поговорить с ними о компьютерах, ответить на их вопросы и удовлетворить любопытство.

2. Всегда сидите за компьютером вместе с детьми данного возраста, когда они подключаются к Интернету.
3. Установите четкие правила по использованию Интернета.
4. Настаивайте на том, чтобы дети не разглашали своей личной информации, например свое реальное имя, адрес, номер телефона или пароли, людям, которых они встречают в Интернете.
5. Если на сайте детей просят указать свое имя, чтобы персонифицировать веб-материалы, помогите детям придумать псевдоним для работы в Интернете, который бы не выдавал никакой личной информации.
6. Используйте средства семейной безопасности для создания соответствующих профилей для каждого члена семьи, а также для обеспечения фильтрации интернет-содержимого.

Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузерInternet Explorer.

7. Все члены семьи должны показывать пример детям, которые только начинают пользоваться Интернетом.

От 11 до 14 лет

В этом возрасте дети хорошо разбираются во всех вопросах, связанных с Интернетом, однако все равно рекомендуется следить и контролировать их, чтобы оградить детей от неподобающих материалов. Можно воспользоваться средствами интернет-безопасности, которые ограничивают доступ к содержимому и сайтам, а также предоставляют информацию о действиях в Интернете. Проследите за тем, чтобы дети в этом возрасте понимали, какую личную информацию не следует разглашать в Интернете.

Постоянно находиться рядом с детьми в этом возрасте, чтобы контролировать их использование Интернета, практически нецелесообразно. Можно использовать следующие средства: Функции семейной безопасности Windows Live, средства родительского контроля Windows 7и Windows Vista.

Советы по безопасности, которые следует учитывать при подключении к Интернету вместе с ребенком в возрасте **11-14** лет:

1. Важно формировать открытое и позитивное общение с детьми. Поговорите с ними о компьютерах, ответьте на их вопросы и удовлетворите любопытство.
2. Установите четкие правила по использованию Интернета.
3. Настаивайте на том, чтобы дети не разглашали своей личной информации, например свое реальное имя, адрес, номер телефона или пароли, людям, которых они встречают в Интернете.
4. Если на сайте детей просят указать свое имя, чтобы персонифицировать веб-материалы, помогите детям придумать псевдоним для работы в Интернете, который бы не выдавал никакой личной информации.
5. Используйте средства семейной безопасности для создания соответствующих профилей для каждого члена семьи, а также для обеспечения фильтрации интернет-содержимого.
6. Настройте средний уровень в средстве семейной безопасности, который накладывает некоторые ограничения на содержимое, сайты и действия в Интернете.
7. Компьютеры, подключенные к Интернету, следует устанавливать в открытом месте, где можно легко контролировать действия детей.
8. Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер Internet Explorer.
9. Попросите детей рассказать, не ощущали ли они неудобство или страх от уведенного в Интернете или в ходе общения с другими людьми. Проявляйте спокойствие и

напомните детям, что их никогда не накажут за то, что они вам расскажут. Похвалите их и попросите их сообщить вам, если то же самое повторится еще раз.

От 15 до 18 лет
Подростки должны иметь практически неограниченный доступ к содержимому, сайтам или действиям. Они хорошо разбираются с тем, как использовать Интернет, однако родителям все равно следует напоминать им о соответствующих правилах безопасности. Родители всегда должны быть готовы помочь своим детям-подросткам разобраться, какие сообщения являются непристойными, а также избегать опасных ситуаций. Родителям рекомендуется напоминать детям-подросткам о том, какую личную информацию не следует предоставлять через Интернет.

Советы по безопасности, которые рекомендуется выполнять, когда ваши дети-подростки используют Интернет:

1. Старайтесь по-прежнему поддерживать как можно более открытое общение внутри семьи и позитивное отношение к компьютерам. Обсуждайте с детьми их общение, друзей и действия в Интернете точно так же, как другие действия и друзей.

Просите детей-подростков рассказывать вам, если что-то или кто-то в Интернете доставляет им чувство неудобства или страха. Если вы подросток и вам не нравится что-то или кто-то в Интернете, расскажите об этом.

2. Создайте список семейных правил использования Интернете дома. Укажите виды сайтов, которые можно посещать без ограничений, время подключения к Интернету, расскажите, какую информацию не следует разглашать в Интернете, а также предоставьте инструкции по общению с другими в Интернете, включая общение в социальных сетях.
3. Компьютеры, подключенные к Интернету, должны находиться в открытом месте, а не в спальне ребенка-подростка.
4. Изучите средства фильтрации Интернет-содержимого (такие как Windows Vista, средства родительского контроля Windows 7 и Функции семейной безопасности Windows Live) и используйте их в качестве дополнения к контролю со стороны родителей.
5. Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер Internet Explorer.
6. Следите за тем, какие сайты посещает ваш ребенок-подросток и с кем он общается. Просите их пользоваться контролируемыми чатами, настаивайте на том, чтобы они использовали только общедоступные чаты.
7. Настаивайте на том, чтобы они никогда не соглашались на встречу с друзьями, с которыми они познакомились в Сети.
8. Научите детей не загружать программы, музыку или файлы без вашего разрешения. Обмен файлами и использование текста, изображений или рисунков с веб-сайтов может привести к нарушению авторских прав и может быть незаконным.
9. Поговорите со своими детьми-подростками о содержимом в Интернете, предназначенном для взрослых, и порнографии, а также укажите им позитивные сайты, посвященные вопросам здоровья и сексуальности.
10. Помогите им защитить себя от спама. Проинструктируйте своих детей-подростков никогда не давать свой адрес электронной почты при общении в Интернете, не отвечать на нежелательные почтовые сообщения и пользоваться фильтром электронной почты.

11. Знайте, какие сайты ваши дети-подростки посещают чаще всего. Убедитесь, что ваши дети не посещают сайты, содержащие оскорбительные материалы, и не публикуют свою личную информацию. Следите за тем, какие фотографии публикуют ваши дети-подростки и их друзья.
12. Учите своих детей отзывчивости, этике и правильному поведению в Интернете. Они не должны использовать Интернет для распространения сплетен, клеветы или запугивания других.
13. Проследите за тем, чтобы дети спрашивали у вас, прежде чем совершать финансовые операции в Интернете, включая заказ, покупку или продажу товаров.
14. Обсудите со своими детьми-подростками азартные игры в Интернете, а также потенциальные риски, связанные с ними. Напомните им о том, что азартные игры в Интернете являются незаконными.

- Конфиденциальность в Интернете
- Персональные данные онлайн
- Репутация в сети
- Защита Персональных данных